10 April 2024

EUCS: Ensuring full transparency and protection for European cloud users' most sensitive data is critical

A joint action from European Cloud Providers and Users

Deliberations on the candidate EU cybersecurity certification scheme on cloud services (EUCS) have been ongoing since December 2019. Much of the discussions have been centered around the inclusion of immunity / sovereignty requirements. **As European cloud providers and users committed to EU's digital competitiveness, we have been consistently advocating for the integration of transparent and harmonized requirements at the highest evaluation level of the EUCS scheme to protect the most sensitive European data against unlawful access**. Keeping in mind that EUCS is conceived as a voluntary certification scheme, we believe it should be grounded in existing market practices and user preferences while bringing transparency and protection to users where needed.

We believe the inclusion of sovereignty requirements is necessary to overcome market fragmentation, protect European organizations' most sensitive data, and encourage the development of sovereign cloud solutions in Europe. **Removing any reference to sovereignty provisions from the main scheme (including if shifted to an International Company Profile Attestation, ICPA) clearly fail to meet these objectives.** This would not only contradict what has been proposed in the previous EUCS schemes for over two years, but also give up the collective efforts undertaken by ENISA, the European Commission and Member States' representatives**.** The EU must not abandon its overall objective of fostering digital sovereignty, a goal that is all the more relevant in a context of geopolitical uncertainty.

We therefore urge Member States to reject any proposals that remove sovereignty requirements from the main body of the EUCS scheme for the following reasons:

1. **Addressing the risk of unlawful data access:** the inclusion of EU-HQ and European control requirements in the main scheme is necessary to mitigate the risk of unlawful data access on the basis of foreign laws, incompatible with the GDPR. The removal of these criteria from the main body of the scheme (including from a potential level high+/EL-4) means that adherence to EU sovereignty is no longer required for certification and that all cloud providers can potentially be certified at the highest security level of EUCS, even if they are subject to extraterritorial legislation (e.g. Chinese National Intelligence Law or US CLOUD Act). The result is that the risk of unlawful access remains unaddressed by the certification itself.
2. **Ensure consistency across the EU market:** harmonization of sovereignty requirements in Europe can only be achieved by setting out a uniform set of provisions in the main body of EUCS, enhancing clarity and consistency across the European market. Shifting this responsibility to national procurement officers (e.g. as suggested in the Belgian's Center for Cybersecurity concept note) who are supposed to decide for themselves which 'sovereignty elements' they deem necessary (or not) will inevitably lead to fragmentation. Contrary to the objective of EUCS, i.e. to bring more harmonization, the result will be different requirements at national level and, consequently, legal, technical, and economic uncertainties for both EU cloud providers and users in the implementation of their cloud strategies.
3. **Offering users' clarity and transparency:** cloud users require transparency about the level of protection of their data. There is a high likelihood that users will rely on the certification scheme to ensure that their data is adequately secured. However, if a future EUCS scheme will leave the risk of unlawful data access unaddressed, this may lead to situations where cloud users will simply rely on the highest level without being adequately protected or informed about the risk of unlawful

access stemming from extraterritorial legislation. This will ultimately impede investments in sovereign cloud solutions.

Including a clear and uniform set of sovereignty requirements in the main body of the EUCS is fundamental to support transparency, user choice, and the availability of alternative cloud solutions that are built in conformity with sovereignty requirements. On the contrary, **removing such requirements from the scheme would seriously undermine the viability of sovereign cloud solutions in Europe – many of which are either in development or already available on the market**. It would also impede European customers from being able to identify with certainty sufficiently secure solutions for their sensitive applications.

Moreover, it would be **inconsistent with European legislation such as the recently adopted Data Act[1] and important initiatives such as Gaia-X**. The GAIA-X policy rules, which were inter alia designed to ensure data sovereignty, explicitly include both an EU-HQ (criterion P5.1.4) and European control (criterion P5.1.5) requirement at the highest assurance level (label level 3). GAIA-X therefore sets a blueprint for EUCS, one that was jointly developed and adopted by cloud providers and users in Europe.

We therefore urge policymakers to take the necessary time to fully take into account the implications of a potential removal of sovereignty provisions from the main body of the EUCS scheme for European cloud providers and users as well as for the protection of Europe's most sensitive data as a whole. A digital and sovereign Europe requires access to the best cloud technologies while supporting the development of sovereign cloud solutions in Europe. We do believe these two goals can go hand in hand by supporting the inclusion of a harmonized set of sovereignty requirements in the framework of a voluntary EUCS scheme.

Sincerely,

A1, Airbus, Aruba S.p.A., Capgemini, Dassault Systemes, Deutsche Telekom, EDF, Exoscale, Gigas, Ionos SE, OpenNebula Systems, Orange, OVHcloud, Proximus, Eutelsat Group, Sopra Steria, StackIT, TIM.


[1] Art. 32 of the Data Act includes a prohibition of unlawful international governmental access and transfer regarding non-personal data, https://eur-lex.europa.eu/eli/reg/2023/2854

Annex

Background

In its Impact Assessment accompanying the proposal for the Data Act, the European Commission noted that 'unlawful access by non-EU/EEA governments to data stored in the cloud' represents **one of the most problematic drivers behind the lack of trust in cloud solutions**. This was confirmed by the consultation on the Data Act, where **76% of respondents** (business organisations and associations) indicated that they **perceive access to data by foreign authorities as a risk** to their organization[2].

Consequently, the **Data Act**, which has entered into force in January 2024, is aiming to **protect non-personal data (e.g. trade secrets) against unlawful access**. However, while the Data Act has defined a general requirement for cloud providers regarding the handling of non-personal, there is **still a lack of harmonized requirements** for cloud service providers (CSP) to demonstrate their compliance with EU law. Moreover, the risk of unlawful data access not only affects non-personal but also personal data.

Already in 2021, the then **Chair of the European Data Protection Board, Andrea Jelinek**, had called for the integration of specific requirements in the EUCS in a letter sent to the Executive Director of ENISA. In this letter, Ms Jelinek notes that "*offering an assurance level of the EUCS with strong guarantee that the cloud service provider is not subject to foreign access incompatible with the GDPR would facilitate the compliance of processing activities relying on cloud services certified with this level of assurance.* ***Failing to do so would be a missed opportunity to foster security and compliance across Europe***."[3]

Against this backdrop, a proposal was included in the EUCS that aims to protect European data from unlawful access. The political discussions on the EUCS have been stalled due to disagreements regarding the inclusion of these requirements. In particular, the so-called 'EU-HQ' and 'European control' provisions have been a focal point of these discussions.

It is important to remember that EUCS is conceived as a **voluntary certification scheme**. Its main goal is to harmonise security requirements for cloud services in the EU, thereby giving both cloud providers and users visibility on the security level of a given service. Requirements to protect against unlawful access would be predominately reserved for the **highest assurance level** of the certification scheme, which is **foreseen as an additional option for the most sensitive categories of data** (e.g. certain public sector data, health related data).

Therefore, EUCS is not unduly restricting access to the market for cloud services in the EU. The **vast majority of cloud services in the EU would remain unaffected**. Instead, EUCS could define different security levels in the scheme, giving cloud users visibility and options to choose from depending on their needs. It is expected that the highest assurance level will be mainly targeted at use cases with highly sensitive data, for which protection against unlawful access is often a **precondition for cloud uptake**.

Finally, the EU's proposal on cloud certification is also not unprecedented. A similar approach is taken for example by the **US government**, when it comes to the **cloud use of US agencies**. The **Federal Risk and Authorization Management Program (FedRAMP)** provides for an in-depth security assessment and authorization for cloud services used by US agencies, which may include detailed **reporting on foreign ownership of cloud providers**, **disclosure of foreign elements** of supply chains, and applicable **geolocation restrictions** for provided products and services.

---

[2] https://digital-strategy.ec.europa.eu/en/library/public-consultation-data-act-summary-report

[3] https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-enisa-regarding-european-cybersecurity_hu

European cloud providers and users have been long advocating for the inclusion of requirements to protect European data against unlawful access at the highest certification level of EUCS. The **European control and EU-HQ provisions** are central to such requirements, as they ensure that an EU-based company acts as the main cloud provider towards the customer in cases where this may be desirable.

This is necessary for the following reasons:

- Extraterritorial legislation such as the US CLOUD Act[4] applies directly to non-EU cloud providers that fall under the respective jurisdiction. In the example of the US CLOUD Act, this means that US authorities can access data from US cloud providers, even if such data is stored within the EU. The **possibility of extraterritorial access** means that **data localization measures alone are insufficient** to prevent unlawful data access.
- If an EU based company acts as the main cloud provider, the exposure to extraterritorial legislation can be reduced. While non-EU providers remain subject to extraterritorial legislation even if such legislation conflicts with EU law, **EU providers can act as trusted partners** to ensure data is processed in **compliance with national and EU law**.
- The **European control and EU-HQ provisions are therefore essential**, as they put EU cloud providers in the driving seat, mitigating the exposure of European data to extraterritorial legislation and with it the risk of unlawful access. This is also the reason why the **GAIA-X policy rules**, which were designed to ensure data sovereignty, explicitly include both an EU-HQ (criterion P5.1.4) and European control (criterion P5.1.5) requirement at the highest assurance level (label level 3)[5]. **GAIA-X therefore sets a blueprint for EUCS**, one that was jointly developed and adopted by **cloud providers and users in Europe**.
- Contrary to some beliefs, the above-mentioned **conflict of laws cannot be solved through an adequacy decision of the EU**. The latter only applies to personal data that is being transferred from the EU to the US for further processing or storage. It does not address the issue of unlawful access from US law enforcement authorities to data stored in the EU. Neither does it apply to non-personal data which can also be subject to unlawful access (see Data Act).
- Both the GDPR (Art. 48) as well as the US CLOUD Act **require a separate international agreement to deal with law enforcement requests for data**. Such an agreement between the EU and the US is being negotiated for several years but **has not been finalized or adopted as of today**. Even if adopted, it would likely take more time to implement, given the necessary lead time needed to put in place and adapt the technical systems needed.
- Proposals that would foresee a complete removal of the EU-HQ and European control criteria (incl. on EL-4) therefore **do not meet the requirements needed to effectively limit exposure to extraterritorial legislation**. In reality, these attempts would **water down the certification rules** and allow cloud providers to be certified at the highest level while the issue of **unlawful access remains unaddressed**.

Therefore, without the EU-HQ and European control requirements, the EU would give up its most effective instrument to mitigate the risks of unlawful data access. As a consequence, **cloud users** who cannot or do not want to run the risk of unlawful access continue to be **left without real alternatives and a clear framework that supports their needs**. At the same time, it would **seriously undermine EU cloud providers' efforts to invest in sovereign cloud solutions**.

[4] Other examples mentioned in the Impact Assessment on the Data Act: Executive Order 12333 (US), Section 702 of the Foreign Intelligence Surveillance Act (FISA) (US), the 2017 National Intelligence Law (China) and more.

[5] https://docs.gaia-x.eu/policy-rules-committee/policy-rules-labelling/22.11/