Survey of the potential impact of PUA/INL criteria in the EUCS on the Dutch Cloud market

Online Trust Coalition

Introduction

In 2019 the EU Cybersecurity Act (Regulation EU 2019/881 of 17 April 2019) went into effect. This regulation appoints ENISA as the European Union Agency for Cybersecurity (Title 2) and provides a Cybersecurity Certification Framework (Title 3) for ICT products, ICT services and ICT processes. Within the context of this Cybersecurity Certification Framework the European Commission requests ENISA to prepare candidate Cybersecurity Certification Schemes. These schemes are prepared under the direction of ENISA by Ad-hoc working groups composed of experts (including specialists, stakeholders and government representatives). One of the first schemes to be produced is a scheme for cloud services.

The development of the cloud services scheme (the EUCS) started in early 2020 and a first draft was published for public consultation in December 2020. After the public consultation the criteria section was significantly revised, and both the criteria and the conformity assessment methodology were submitted for review to CEN/CENELEC. Separate from the revised criteria, ENISA, at the direction of the European Commission, added an Annex J to the scheme. This annex contains additional requirements to safeguard cloud services that are certified for assurance level HIGH, against unlawful (not in compliance with EU-Law) access. These are so-called PUA-criteria: Protection of European Data against unlawful access, formerly known as INL-criteria: Immunity for Non EU Law.

Various parties criticize these PUA/INL-criteria as they fear these criteria will significantly impact the European market for cloud services. PUA/INL-criteria effectively block access to the EU cloud market for assurance level HIGH certified services from non-EU providers who currently are dominant in this segment. Additionally, the impact for EU-providers that use non-EU services as part of their services will be significant.

In the opinion of the Dutch government the decision to include the PUA/INL-criteria in the final scheme is a political discussion that should include an economic impact assessment. The Netherlands submitted this view in a non-paper to the EU member states. This paper was signed by various member states. However, France persists in including the PUA/INL-criteria in the scheme for assurance level HIGH certification. The European Commission supports France in that they do not see a need for an economic impact assessment.

To validate the importance of an economic impact assessment the Dutch Ministry of Economic Affairs and Climate Policy asked the core team of the Online Trust Coalition to perform a survey under Dutch professional users and providers of cloud services. The objective of this survey is to assess whether a major impact can be expected. The survey process started in 2022 with

interviews among providers of cloud services and was finalized in 2023 by interviewing cloud users. The “Market study into cloud services” report published in September 2022 by the Dutch Authority for Consumers and Markets (ACM) was also included in this survey.

Most important findings

- Both interviews with providers and users of cloud services show absence of detailed understanding of the EUCS and PUA/INL-criteria. Moreover, many questions exist on new and future EU regulations relating to cloud services like NIS2, Digital Markets Act, Digital Services Act, Data Act, Digital Operational Resilience Act and the Cyber Resilience Act. As a result, organizations are not sure how to design their systems, services and processes in order to be adequately prepared for these regulations. Evidently, both providers and users of cloud services are currently not prepared.

- Users of cloud services in general in the long run are in favor of having provisions that safeguard compliance with EU law when carefully implemented in regulations and applicable to all providers. Users of cloud services stress that non-EU providers should be able to comply with these provisions and allowed time to do so. Denial of access to the EU market for non-EU providers will lead to important negative side-effects, such as limitations in development of services and products, increase in cost compared to competitors in the market, lack of certain (cybersecurity) functionality that is essential for delivering secure services, etc.

- Although Cybersecurity Certification based on the Cybersecurity Act is voluntary, parties expect the aforementioned regulations to mandate certification for critical services and services procured by government (related) bodies in the future. Providers expect that assurance level HIGH certification of their services will be required to have a chance of winning tenders. Their assessment is that assurance level HIGH certification will become the standard for cloud services in the EU.

- The previous point will cause tension in the EU market for cloud services. SME providers risk losing their business cases due to the high cost of certification, which will lead to a reduction in the number of providers and services available in the market. Providers that do survive will be faced with higher costs and as supply reduces the prices of cloud services will increase.

- The question arises if the PUA/INL-criteria will result in banning currently dominant, mostly US, providers from the EU cloud market. For these global players, the EU cloud market is very significant. They will therefore seek ways to circumvent the PUA/INL-criteria to continue to offer their products and services in the EU market. These global payers estimate that prices for their services will increase by at least 25% as a result.

- At the market level the question arises about what will happen if access to the EU market is restricted for non-EU providers. Currently the most advanced and innovative services, like AI, are provided by US providers. If availability in the EU market of these technologies becomes less, EU providers are faced with the challenge to develop these themselves. Currently there is a gap between the innovative capabilities of EU

and US providers. Additionally, a relation exists between funds available for the development of these technologies and market share: the bigger the market share, the higher the funds available for innovation. Assessment is that this market share can only be achieved on a global scale where EU providers must compete with US providers that are currently dominant in the global market. This requires EU providers that operate on a scale equivalent to parties like Microsoft, Google and Amazon. Such providers are currently not available in the EU. The question is: will EU providers be able to close the gap or will the gap increase, resulting in the EU falling behind in innovation?

- Both users and providers expect to face migrations as a direct result of including PUA/INL-criteria. For migrating cloud services transparency, interoperability and portability are important success factors that are currently lacking in the market. Especially professional users currently experience technical and economic lock-in with their current suppliers. The ACM report shows an increase in the use of cloud services in the Netherlands: in 2021 use of cloud services by enterprises in the Netherlands rose by 12,2% from 53% to 65%. This is significantly higher than in France where use of cloud services rose from 27% to 29% in 2021. CIOs complain about lock-in issues: migrating to a different provider is challenging and existing providers misuse this by charging extreme prices when renewing contracts or adding new features to existing contracts. CIOs fear that the financial impact of migration due to PUA/INL-criteria will be significant.

Conclusions and recommendations

- Overall expectations are that the impact of including PUA/INL-criteria in the EUCS will be high.
- This applies to individual enterprises (both users and providers) that will be confronted with migration costs, price increases and in some cases even discontinuity of their enterprise.
- This also applies at the market level for the relation between demand and supply and innovation power.
- A detailed forecast is difficult to achieve though due to a lack of detailed insights into the relation between PUA/INL-criteria, other regulations and market response.
- It is clear, however, that both the cloud market and individual enterprises are currently not able to absorb the impact of the PUA/INL-criteria.
- Based on these conclusions we recommend:
    - To perform an EU wide assessment of the impact of PUA/INL-criteria on both the level of the cloud market and individual enterprises, taking into account the effects of new regulations;
    - To define potential scenarios based on this assessment and validate these scenarios against individual assessments by stakeholders and the objectives of EU's Digital Agenda;
    - To detach the implementation of PUA/INL-criteria from finalization of the EUCS scheme, in order to allow sufficient time for the market to prepare and no longer delay implementation of the EUCS.