ONLINE TRUST COALITION

POSITION PAPER ON REGULATORY DEVELOPMENTS AT ENISA ORIGINATING FROM THE CYBER SECURITY ACT

November 26, 2021

The Online Trust Coalition (OTC) follows the current regulatory developments with respect to the Cyber Security Act (CSA), and the work done by ENISA to achieve a common, harmonized approach for cyber security of cloud services in the European Union (EU).

With respect to the topic at hand, we recognize the following ambitions of the European Commission (EC)[1]:

- Improve both our data- and digital sovereignty by restoring the balance in the European market of cloud services.
- Strengthen the EU cloud market by promoting the sharing of data, data portability and innovation of cloud services.
- Harmonize rules and regulations for the cyber security of cloud services; to effectively protect the data of EU citizens and organizations, to create a level playing field and to achieve assurance for- and trust in cloud services for a multitude of stakeholders.
- Strengthen the EU's DSM (digital single market) by enabling the free flow of data and removing regulatory barriers.

Given the speed of market developments and the EU's digital ambitions and substantial market imbalance, the OTC shares the sense of urgency of the EC. The OTC is therefore actively cooperating on various levels to make these ambitions a reality. For example, the OTC is involved in the Gaia-X project and is committed to making Gaia-X a success. Additionally, the OTC is involved in the international standardization efforts through participation in working groups organized by the *Netherlands Normalisation Institute* (NEN), and the *Comité Européen de Normalisation Electrotechnique)* CENELEC.

We have observed several developments that, if not addressed, will put the aforementioned objectives at risk. These developments are:

1. ENISA's regulatory approach towards cyber security for cloud services fails to achieve its goals and introduces problems

Existing EU regulations that affect the cybersecurity of digital services, such the GDPR, the NIS, DORA[2] and the future AI regulation, share a risk-based, and principle-based regulatory approach. The idea is that organizations must perform an analysis of risks for the services or data processing subject to the regulation, then implement appropriate and effective controls and measures to mitigate these risks. This approach leaves organizations room to use best-of-breed

[1] https://ec.europa.eu/info/sites/default/files/ec_cloud_strategy.pdf, https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4919, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

technologies and processes, and allows organizations to adapt their risk mitigation strategy: i.e. their governance, technologies and measures, to the continuously changing risks, threats, challenges, insights and technological innovations. Not the rules, but the desired results prevail.

Following the CSA's mandate, ENISA is currently developing the European Cloud Services Scheme (EUCS)[3], with harmonized cyber security requirements of cloud services. The EUCS is however not based on the common risk- and principles based approach, but uses a product- and predominantly rule-based regulation strategy. This has significant negative impact on the market. Worse, ENISA's approach is detrimental to agility and innovation for European Cloud Service providers (CSP's) and it also exacerbates the market's problems with respect to achieving assurance for cloud consumers.

- **A rule-based approach does not provide sufficient assurance.**
  Applying generic, static rules to mitigate risks in a fundamentally dynamic environment such as a cloud service does not guarantee that cyber security risks are sufficiently mitigated. Furthermore, the static nature of product- and rule-based regulation prevents CSP's from adapting their risks mitigation strategies to continuously changing challenges and limits their options to implement cyber security innovations. Third, such a certification does not verify if the measures (rules) are suitable for mitigating the specific risks in the specific context for which the cloud service is intended, i.e. if the objectives of effective security risk mitigation are met.
- **It reverses effective and accepted assurance solutions provided by the market.**
  Rather than relying on one-time certifications of rule-based schemes, cloud consumers (such as enterprise CIO's, Banks, insurance companies, the public sector) increasingly seek assurance by routinely demanding effectiveness audits on the cloud services they depend on, originating from their right to audit in the GDPR and other EU regulations. The demand for additional audit procedures is generally higher in case of rule-based schemes than in case of audits performed under [4]. One of the reasons for this is that financial regulators are aware that circumstances (such as risks) of a cloud service continuously change, and that certification of a rule-based governance model cannot provide the assurance they require.
- **ENISA's approach conflicts with the GDPR and DORA**
  The rule-based approach for cyber security leads to a fundamental mismatch with the GDPR and DORA. These regulations require a risk-based approach towards cyber security, with adequate risk analyses and the implementation of principle-based governance schemes to mitigate risks.
- **It increases audit pressure and introduces enormous cost for CSPs**
  ENISA has attempted to compensate for the dynamic nature of cloud services by introducing a large amount of rules. Typical cyber security frameworks that are common in the market have approximately 100 controls, ENISA's EUCS has over 550 controls. Consequently, the compliance cost for EU small and medium-sized enterprises (SME) providers for the EUCS certification is huge. Participants in the first pilots with the new ENISA cloud scheme estimate the annual cost for just the EUCS certification between €200.000 and €250.000. And because

[3] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[4] https://www.iaasb.org/publications/staff-overview-international-standard-assurance-engagements-isae-3402-assurance-reports-controls

the EUCS certification does not provide sufficient assurance, Cloud consumers will continue to demand additional assurance audits, which results in a further increase of the audit pressure and compliance cost.

Further background and explanation, and effects of the rule- versus principle-based approach can be **found here**[5].

2. Member states opt for inclusion of sovereignty rules without foundation in political decisions.

Several stakeholders in the ENISA working groups have expressed their concerns about the lack of protection of personal data of EU citizens. The background is the decision of the Court of Justice of the European Union which invalidated the privacy shield, but companies struggle with the practical consequences. Such as cease their data transfers to third countries, which practically means that certain cloud services can no longer be used. These data sovereignty concerns were expressed in a non-paper submitted by France, Germany and several other member states, in which they propose the inclusion of specific sovereignty provisions in the highest risk-class in the EUCS. Such as mandatory data-localization (i.e. requirements for the physical location of hardware) in the respective member states[6]. The risk-class "high", as defined in the CSA, is intended for special, exceptional cases, hence the impact of such specific rules is estimated to be marginal.
But in practice such rules have substantial impact on the market. The reason is that in practice cloud consumers demand nothing but the highest possible protection for sensitive data, which translates to a demand for the highest level of data protection by suppliers. The market reflects this: there is neither demand nor a market for services that do not claim to offer the highest possible cyber security and reliability. Consequently, such rules affect everything. It can easily result in the exclusion of suppliers, staff and services from suppliers in other member states and/or third countries.

Summarized, specific measures that are being discussed in the technical context of standards for cyber security, turn out to have a substantial effect on sovereignty, on the EU cloud market and even have significant political consequences.
The Netherlands have provided a reaction to the mentioned non-paper[7]. The OTC shares this opinion that it is inappropriate to include detailed regulation in the context of the CSA, (and consequently the NIS) with such a severe impact on the EU digital market without a clear basis in political decisions.
Such regulatory decisions should not be made by ENISA, but must be discussed in a political context, and must be thoroughly evaluated with respect to their impact and consequences first.

[5] https://onlinetrustcoalitie.nl/wp-content/uploads/2021/11/211126_OTC-Rules-vs-Princples-based-regulation-Background_def.pdf
[6] https://onlinetrustcoalitie.nl/wp-content/uploads/2021/11/20210716_Non-Paper-by-DE-ES-FR-IT-on-immunity-in-EUCS_vf.pdf
[7] https://onlinetrustcoalitie.nl/wp-content/uploads/2021/11/NL-opinion-on-the-non-paper-immunity-to-non-EU-law-v1.0-20211007.pdf

3. Local policies may result in a fragmentated EU cloud market

Some member states, for example particular France, have, in anticipation of the outcome of the EU certification process, recently invested in national policies for cloud services[8]. These policies appear to be prohibitive for CSPs from other member states. Although the CSA states that the EU schemes should replace national schemes, we have grave concerns about these developments. We already observe significant changes in the market: some of the larger non-EU players have already invested in partnerships in France, such as cloud services of local suppliers using their technologies, to comply with these data localization requirements[9]. Because, understandably, they want to protect their interests and market share. Such (costly) strategies are however not a feasible approach for SME CSP's in other member states.

Access to all EU markets for EU CSPs is an important principle of the Digital Single Market and easy access to all EU markets is imperative for CSPs to achieve scale. The Commission should take notice of this development and take appropriate steps to prevent further fragmentation of the EU cloud market. This development will otherwise put both the EU cloud strategy, and projects such as Gaia-X at risk.

RECOMMENDATIONS

The OTC recommends the EU commission and ENISA to take the following steps:

- **Embrace the risk-based, and principle-based approach for cyber security of cloud services.**
  ENISA must change its course and restart its cloud certification strategy using a principle-based approach as required by cyber security approach in regulations such as the GDPR and DORA.
  Rather than designing new rules ENISA should create a toolbox with applicable cyber security frameworks for cloud services that are commonly used by CSPs world-wide. In addition, ENISA must invest in selecting (or developing) harmonized EU methods for assurance. This involves the selection and accreditation of audit standards that can verify the CSPs ability to analyze and mitigate risks, such as the commonly used ISAE3402 standard.
  Furthermore ENISA should focus on standards for audit reports and for quality marks for stakeholders that need assurance for cloud services.
  Last but not least, the commission and ENISA must ensure that cloud security requirements will be compatible with other regulations affecting cloud services, such as DORA and the GDPR.
- **Expedite the wider political discussion on data sovereignty and digital markets.**
  The European Commission should complete the wider political discussion on data sovereignty. This includes the relevant perspectives of the GDPR, data autonomy, data sharing, Artificial Intelligence and the NIS since these are all affected and connected. The

[8] https://www.ssi.gouv.fr/en/actualite/european-secure-cloud-a-new-label-for-cloud-service-providers/
[9] https://www.thalesgroup.com/en/group/investors/press_release/thales-and-google-cloud-announce-strategic-partnership-jointly, https://www.tellerreport.com/news/2021-05-29-microsoft-to-allow-orange-and-capgemini-to-exploit-its-cloud-technology---france-24.SkzbRLN19_.html

political discussions about the causes of perceived unlawful data-transfers, the apparent lack of enforcement of the GDPR, about data-sovereignty and access of EU versus non-EU CSPs to the EU market, needs completion and convergence, before any concrete measures or rules can be discussed by the ECCG or can be incorporated in EU-wide cloud certification schemes such as the EUCS.

- **The commission must safeguard and strengthen the Digital Single Market principles for cloud.**
  Ensure easy access to the cloud market of all member states by all EU CSPs; including for services being marked as high-risk, since all co-location and Infrastructure as a Service (IaaS) will de facto end up in this category. This is of vital importance for EU CSP's to achieve sufficient economy-of-scale. Member states must, at this time, refrain from implementing policies that overrule or preempt the EU harmonization and standardization efforts for cyber security. The commission must certify that local security policies that impede access to member states' markets are actually replaced by EU standards. Despite the otherwise valid concerns about digital sovereignty, the Digital Single Market principles should come first.

ABOUT THE OTC

At the initiative of the Dutch Ministry of Economic Affairs and Climate the Online Trust Coalition unites leading organizations from government, industry, science, community and NGO's. OTC's vision, as set out in the September 2020 manifesto[10], is the broad availability of unambiguous, efficient and accessible methods that let cloud service providers prove the reliability, conformity and security of their services; and support Cloud Consumers, i.e. users or customers of a cloud service and other stakeholders with obtaining the assurance they require. OTC's mission is to develop and promote methods and standards for assurance, i.e. the way in which trust is offered, requested, supplied and substantiated[11].

[10] https://onlinetrustcoalitie.nl/wp-content/uploads/2021/09/otc_manifest_en_v8.pdf
[11] https://onlinetrustcoalitie.nl/wp-content/uploads/2021/10/Online-Trust-Coalitie-white-paper-Trust-in-the-Cloud-February-9-2021.pdf