

A world-leading European cybersecurity framework must prioritize cutting-edge encryption technologies

As we live more and more of our lives online, strong cybersecurity protections are vital. Cybersecurity impacts not only our personal safety, but also national security. And the consequences of poor cybersecurity standards can be severe. The 2021 ransomware attack affecting the Irish Health Service Executive, the largest known attack against a health service computer system, is clear proof of this: almost all outpatient and radiology services across the entire country were cancelled for several weeks.

Across the EU, the current fragmented cybersecurity standards and practices make it near impossible to build resilience and effectively combat the growing risks posed by cyberattack. There is therefore a crucial need for more cooperation on cloud-based cybersecurity. In recognition of this, the EU Cybersecurity Act provided the framework for the EU Cloud Certification scheme for cybersecurity (EUCS). The EUCS aims to establish a unified approach to cybersecurity certification in the European internal market and if adopted, can come into effect from 2025.

Yet there are a number of potential pitfalls in the proposed draft of what is ultimately meant to be a technical standard, rather than a political measure. As it stands, the draft could be overwhelmed by sovereignty provisions which ultimately hinder, rather than help, cybersecurity. For example, **requirements for cloud providers to be headquartered within the EU could mean that providers of best in class technologies and leaders in cyber defence are shut out of playing a meaningful role in enhancing European security.**

Exacerbating the impact of these discriminatory measures, the latest draft of the EUCS seems to envisage a much broader scope for these sovereignty provisions than the stated intention of limiting them to national security data-sets alone. **This broad scope of Level High + now risks covering economic data and health data as well as other open-ended categories that may result in large parts of European industry and public services without access to advanced cloud technologies.**

The emphasis placed on **data localization** – the storing and processing of data within a specific geographic location – to safeguard privacy **will also bring significant drawbacks to the security and resilience of systems. It will also disproportionately increase costs for the public and private sectors**, effectively harming innovation and the ability to adequately serve and support users.

Data localization has a role to play in enhancing European governments' control over their citizens' data, and Member States should have the right to certify particularly important resources based on their national regulations, but encryption is the most secure method of data protection available e.g. the Advanced Encryption Standard. **Relying on data localization alone creates single points of physical vulnerability that can increase cyber risk.** When extended to forms of data on cyber threats that are integral to analysis and response to cyber threats, localization forces these data into regional silos where they cannot be cross-referenced within a global context or acted on in a holistic way will severely hinder effective cyber response not only for Europe, but also globally. In addition to physical vulnerability, some EU member states lack the infrastructure to host significant quantities of localized secure data and will struggle to meet the requirements in the EUCS.



Instead of proposing a framework seriously affecting cybersecurity, the EU should instead work with like-minded countries, to develop a common approach to data sovereignty, just like it did with the EU-US Data Privacy Framework. Data flows between Europe and the United States are the biggest in the world and a common framework helped in establishing clear rules for them. Similarly in this case, to ensure that EU citizens' data is protected, also when it is localized outside the EEA, a common set of rules should be established. This way the EU would ensure the security of citizens' data and compliance with the EU law, while developing a scheme that is effective and allows for data transfers to other liberal democracies.

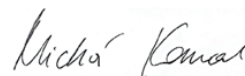
The technical flaws and the conflation of political and cybersecurity policies in EUCS are also subject to a worrying lack of transparency. **Given the lack of clarity around the scope and impact of the sovereignty provisions and the geopolitical dimension driving cybersecurity conversations in 2023, the process lacks wider democratic scrutiny and debate.** Regrettably, the voice of the Member States has been neglected in the process - almost a third of them have expressed concern that these issues are not being addressed in a transparent manner.

Furthermore, there has been no substantive consultation on the scheme since 2021, despite the introduction of a number of material changes, such as the aforementioned sovereignty restrictions on cloud providers. This creates the risk that sweeping changes to European cybersecurity standards could be introduced without proper oversight. This issue has increasingly been raised by Members of the European Parliament who indicated the lack of transparency and the need for greater parliamentary oversight over the adoption of cybersecurity schemes going forward.

Without change, **the sovereignty requirements imposed by EUCS could limit both business and customer choice, slow the pace of migration from legacy technology to cloud-native solutions, and delay Europe's progress towards its ambitious Digital Decade targets.** At a time when the EU strives to reach these targets not only for cloud adoption, but also for technologies like AI that depend on widespread availability of cloud services, EUCS risks harming rather than helping the EU's digital transition.

Policymakers must speak up and ensure the EUCS contains sensible solutions that enhance European cybersecurity, not choose outdated rules that could hinder the most robust technologies and put European citizens at risk.

Michał Kanownik



President of Digital Poland
Association