insurance europe

July 2023

Insurance Europe views on the European Cybersecurity Certification Scheme for Cloud Services (EUCS)

The insurance industry welcomes the goal of ensuring that cloud services meet a minimum set of security and trust criteria throughout the EU to facilitate the resilience of its networks and information systems.

However, the latest draft version of ENISA's candidate EU Cybersecurity Certification Scheme for Cloud Services (EUCS) incorporates "sovereignty requirements" that could significantly reduce cloud offerings in the EU and would be likely to increase the costs incurred by European insurers in adopting cloud services.

According to section J.2.4 of the draft scheme, the objective of the "control requirements" that are proposed is to ensure that certified cloud services are operated only by companies based in the EU. This would require cloud service providers (CSPs) to have their registered head office and global headquarters in an EU member state. This is part of a broader overall objective focused on protecting EU data and making it immune from third-country laws with extra-territorial application.

The introduction of sovereignty requirements that effectively limit the ability of insurers to choose between different CSPs could have significant adverse implications for innovation, competition, cybersecurity and digital transformation capabilities in the sector. Aside from the considerable impact this will have on insurers' overall cloud strategy, there are further practical considerations. For example, reducing the range of CSPs on the market would make insurers less agile and could significantly disrupt their ability to scale cloud resources up or down to respond to fluctuating computing demands or to keep pace with customer needs. In many cases, leveraging the size and scale of large CSPs may actually be part of a more efficient overall security strategy. From a commercial perspective, these restrictions will also have significant impacts for insurers when contemplating their exit strategies, business continuity plans and the transfer/storage of data, as well as whether to opt for multi-cloud or hybrid cloud deployment.

The lack of comparable European alternatives to large US-based CSPs means that the current capacity of the European cloud market is unlikely to be able to meet demand, both in terms of quantity and quality. According to recent estimates from Synergy Research Group, Amazon, Microsoft and Google account for two-thirds of the global cloud market. Moreover, the eight largest cloud providers worldwide (all non-European) cover almost 80% of the market.

Furthermore, there is a strong likelihood that the introduction of sovereignty requirements would lead other jurisdictions to introduce similar requirements in response, potentially even going beyond cloud security certification, leading to increased fragmentation in the market.

In addition, the Cybersecurity Act provides for the mutual recognition of certification schemes with third countries, noting that "each European cybersecurity certification scheme should provide specific conditions for such mutual recognition agreements with third countries" (Recital 105). However, ENISA's own admission about its draft candidate scheme states that, "with the inclusion of requirements on independence from non-EU laws, it is quite unlikely that any form of mutual recognition can be achieved" for the two highest evaluation levels.

It should be noted that European insurers are already subject to requirements on outsourcing to third-party CSPs[1], while the Digital Operational Resilience Act establishes a strict oversight framework for critical ICT third-party service providers that provide ICT services to EU financial institutions, irrespective of where that provider is based. Non-EU cloud providers are therefore already subject to robust requirements when providing services in the EU.

[1] EIOPA guidelines on outsourcing to CSPs and the outsourcing requirements under the Solvency II framework

In its request to ENISA to prepare the candidate scheme, the European Commission stated that it is justified by the need to "stimulate cloud uptake in Europe" as "cloud computing is an underlying technology for any development in technological fields". However, any proposals that restrict the range of cloud offerings available to European businesses is unlikely to contribute to stimulating cloud uptake.

While there may be merit in further exploring the possibility of enhancing Europe's digital sovereignty, this should be a longer-term, political discussion at EU level. Aside from the fact that the European cloud market is not sufficiently mature and that it will take time for European providers to reach the level of technical capability of the US hyperscalers, a cybersecurity certification scheme is not the appropriate mechanism by which to introduce such a policy.

The aim should therefore be to ensure the highest possible level of cybersecurity and to encourage the digital operational resilience of European businesses. Cybersecurity certification should facilitate this by helping companies make informed choices based on the assurance that CSPs meet relevant cybersecurity requirements, without inhibiting the range of available services.

Insurance Europe is the European insurance and reinsurance federation. Through its 37 member bodies — the national insurance associations — it represents all types and sizes of insurance and reinsurance undertakings. Insurance Europe, which is based in Brussels, represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers pay out over €1 000bn annually — or €2.8bn a day — in claims, directly employ more than 920 000 people and invest over €10.6trn in the economy.