Skadden

Cybersecurity and Data Privacy Update

November 30, 2023

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Jonathan Stephenson
Associate / London
44.20.7519.7038
jonathan.stephenson@skadden.com

Lisa V. Zivkovic
Associate / New York
212.735.2887
lisa.zivkovic@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

22 Bishopsgate
London EC2N 4BQ, UK
44.20.7519.7000

Latest Draft of the European Cybersecurity Certification Scheme for Cloud Services — Updates for Non-EU Cloud Service Providers

A recent draft of the EU Agency for Cybersecurity's (ENISA's) European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) reveals what requirements are currently being considered (and what requirements have been lifted) for non-EU cloud service providers (CSPs), according to an unofficially released report.[1] Most significantly, the draft appears to remove the requirement for data localisation, except for CSPs that fall within a new assurance level of "high+." The data localisation requirement, which applied to all CSPs under the previous draft, would have restricted the ability of non-EU CSPs to cater to the European market, and possibly reduced cybersecurity capabilities for EU businesses.

Though certification under the EUCS is voluntary, the NIS 2 Directive[2] (which goes into effect on 15 October 2024) provides EU member states with the option to require essential and important entities[3] to use only EUCS certified Information and Communication Technology (ICT) products, including cloud services. This may require certain CSPs to adopt the EUCS for their regulated customers.

EUCS Background

The EUCS arises from the EU's Cybersecurity Act, which called for ENISA to develop an EU-wide cybersecurity certification scheme to regulate cloud service providers, ultimately for adoption by the European Commission. The EUCS is part of the European Commission's broader strategy to facilitate access to secure and interoperable cloud infrastructure and services for European businesses through standardised cybersecurity requirements.[4] A working group of 20 cloud service stakeholders, including representatives for cloud service providers, customers and conformity assessment bodies, support ENISA. Since public consultation for the EUCS ended on 7 February 2021, there has

[1] This latest draft of the EUCS was leaked by *Politico* in August 2023.

[2] Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[3] Including all organisations that are: (i) essential for economic and societal activities, *i.e.*, energy, transportation, financial operations, health, drinking water, wastewater, public administration/electronic communications and digital infrastructure (*e.g.*, data centres, mobile telecommunications infrastructure and broadband infrastructure) as well as business-to-business ICT management service providers and ground-based infrastructure for the provision of space-based services (*e.g.*, satellite infrastructure); and (ii) categorised as important, *i.e.*, providers of digital services, postal and courier services, waste management services, manufacturing services, food distribution services, research services and health care products.

[4] At the European Commission's request (as further set out in the EU Cybersecurity Act (881/2019)), ENISA is also developing (i) an initial draft of European Cybersecurity Certification Scheme for 5G (EU5G) and (ii) the European Cybersecurity Certification Scheme on Common Criteria (EUCC), covering ICT security products (*e.g.*, firewalls, encryption devices, electronic signature devices) and ICT products with built-in security functionality (*e.g.*, routers, smartphones, bank cards). The EUCC is well developed and near adoption.

Latest Draft of the European Cybersecurity Certification Scheme for Cloud Services — Updates for Non-EU Cloud Service Providers

been ongoing debate about ENISA's proposals to impose restrictions on non-EU CSPs. This is of particular importance because, though CSPs only comprised 16% of the European cloud market share in 2020,[5] business adoption of cloud services continues to grow, and public cloud services spending in Europe is anticipated to reach an annual growth rate of 20% and $29 billion (£23.9 billion) by 2027.[6]

ENISA is expected to officially submit the EUCS for feedback to the European Cybersecurity Certification Group (ECCG), comprised of representatives from national cybersecurity certification authorities (*e.g.*, the German National Cybersecurity Certification Authority (NCCA) and the French Agence nationale de la sécurité des systèmes d'information (ANSSI)). Following ECCG's feedback, the European Commission will publish the EUCS to collect final public comments before adopting the scheme.

"High+" Assurance Level To Limit Data Localisation Requirement to Narrower Category of CSPs

The latest draft of the EUCS details the requirements that a CSP operating in the EU would need to comply with in order to achieve one of four certification "assurance" levels for its cloud services. These assurance levels (basic,[7] substantial,[8] high[9] and high+), which are determined by the level of risk associated with the intended use of the cloud service and the level of sophistication of the potential threat actor,[10] impose more or less demanding requirements on a provider depending on the location of the data and the CSP and on governing law.

ENISA's previous proposals applied the more onerous of these requirements (most notably, data localisation) to Assurance Level 3 ("high"), which cloud stakeholders considered to be inappropriately broad. The leaked EUCS draft demonstrates that ENISA responded to these concerns by introducing a narrower category of CSPs with an Assurance Level 4 ("high+") and limiting the controversial data localisation requirement to this new category. Specifically, Assurance Level 4 would apply to mission-critical data and systems that (i) relate to a fundamental interest in society or process particularly sensitive personal or nonpersonal data, and (ii) if breached are likely to result in a threat to public order, public safety, human life or health or the protection of intellectual property rights, *e.g.*, significant reputational or competitive advantage losses.

Recent EUCS Draft Reportedly Maintains Rigorous Requirements for All Non-EU CSPs

Though the leaked EUCS draft limits data localisation requirements to CSPs with a Level 4 Assurance Level, the draft maintains rigorous requirements for all non-EU CSPs. For example, all CSPs, regardless of their assurance levels, must include the law of an EU member state as the governing law and jurisdiction for their procurement contracts with their customers. Furthermore, those with Assurance Levels 3 and 4 must protect against non-EU laws applying to customer data, and only allow employees located in or supervised by an individual located in the EU to provide cloud services.

Assurance Level 4 maintains the most rigorous of requirements, including obligations to:

- Maintain all processing and storage locations within the EU, with limited exceptions.[11]
- Maintain a registered office and global headquarters in the EU.
- Use only trusted services (*i.e.*, services allowing parties to make binding decisions, *e.g.*, electronic signatures) that are provided by a qualified and trusted service provider established in the EU.
- Implement technical and organisational measures to ensure only investigation requests issued under EU law or EU member state law are recognised.

[5] European Commission, 2023 Report on the State of the Digital Decade.

[6] International Data Corporation (IDC), Worldwide Software and Public Cloud Services Spending Guide (V2 2023).

[7] The basic assurance level covers cloud services for low impact, noncritical data and systems, *e.g.*, website hosting and public information, but not platform or infrastructure capabilities. The limited requirements are intended to prevent unsophisticated cybersecurity attacks, *i.e.*, a single person with limited skills and resources.

[8] The substantial assurance level covers cloud services for moderate impact, business-critical data and systems, *e.g.*, confidential business data, email, customer relationship management systems and personal data. This is intended to be the most common assurance level and the requirements are designed to prevent standard cybersecurity attacks, *i.e.*, a small team of individuals with hacking abilities and access to various hacking techniques, including social engineering, but limited resources.

[9] The high assurance level covers cloud services for high impact, mission-critical data and systems, *e.g.*, highly confidential business data and patents. The robust requirements are designed to prevent sophisticated cybersecurity attacks, *i.e.*, a team of highly skilled individuals with access to significant resources, which may be state-sponsored.

[10] Article 52(1), EU Cybersecurity Act (881/2019).

[11] Cloud services must be operated and maintained in the EU, except (a) for certain documented support activities; and (b) if contractually agreed by the relevant customer (excluding any administrative or supervision activities, *e.g.*, relating to the maintenance of a functional component use to provide the cloud service). However, a CSP must offer its customers the option to have all cloud service activities performed in the EU.

Latest Draft of the European Cybersecurity Certification Scheme for Cloud Services — Updates for Non-EU Cloud Service Providers

EUCS Implications for Non-EU CSPs in the EU and UK

We have increasingly seen initiatives from CSPs to introduce EU-specific cloud offerings, including the recently announced AWS European Sovereign Cloud. However, these initiatives will only partially meet the EUCS requirements for Assurance Level 4. Setting up global headquarters in the EU for existing large non-EU CSP players, for example, would require significant and costly business reorganisation. The new requirements may result in those CSPs revisiting some of their cloud services offerings in the EU. Although the proposed scheme will create opportunities for EU CSPs, it may also further delay the European Commission's 2030 target for 75% of EU businesses to adopt cloud, AI and large data processes.[12]

EUCS certification will not apply to any cloud services operated in the UK following its exit of the from the EU on 31 January 2020. The UK does not yet have an equivalent to the EUCS, and the UK National Cyber Security Centre places the responsibility on customers to ensure their CSPs comply with internationally recognised cybersecurity standards (*e.g.*, SOC 2 and ISO 27001) based on the UK National Cyber Security Centre's high-level principles for CSP selection.[13]

[12] European Commission, 2023 Report on the State of the Digital Decade.

[13] UK National Cyber Security Centre, Cloud Security Guidance (version 2.1).