Council of the European Union
General Secretariat

Brussels, 02 December 2022

WK 10666/2022 REV 3

LIMITE

TELECOM

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Revised non paper of Denmark, Estonia, Finland, Greece, Ireland, Latvia, Lithuania, Poland, Slovakia, Sweden and The Netherlands : Perspective on cloud certification and data sovereignty under the Cybersecurity Act

Delegations will find in annex a revised non paper of Denmark, Estonia, Finland, Greece, Ireland, Latvia, Lithuania, Poland, Slovakia, Sweden and The Netherlands : Perspective on cloud certification and data sovereignty under the Cybersecurity Act

Perspective on Cloud certification and data sovereignty under the Cybersecurity Act

by Denmark, Estonia, Finland, Greece, Ireland, Latvia, Lithuania, Poland, Slovakia, Sweden and The Netherlands

Introduction

Cybersecurity is an essential precondition for the successful digital transition of our economy and of our society. The European Union has taken important steps to increase cybersecurity and trust in digital technologies. The Cybersecurity Act and the cybersecurity certification schemes being developed under this Act are an important and necessary part to achieve this.

Recently, the European Commission has asked ENISA[1] to add sovereignty requirements to the European cloud certification scheme. These requirements would apply to cloud service providers which are operating on the European market and would amongst other things ensure that only the EU law applies to these cloud service providers and that maintenance, operations and data must be located within the EU. It is our understanding that the European Commission intends to continue integrating those requirements in the candidate cloud certification scheme while several Member States and cloud service providers have expressed serious concerns. Instead, we propose that this topic will be put on the agenda of the Council. This non-paper: (1) sets out concerns regarding the current proposal, (2) argues for a political discussion before moving forward, and (3) offers guiding principles for the way forward.

1. Strong concerns by cloud service providers and Member States

Our cloud service providers have recently shared clear concerns with regard to the proposed requirements on data sovereignty in the cloud certification scheme, which we would like to highlight. The cloud service providers voice concerns that the proposed data sovereignty requirements will have far-reaching consequences for all cloud service providers (from hyperscalers to SME's[2]). Even when the proposed requirements would only apply to assurance level high[3], and even when in principle certification under the Cybersecurity Act is voluntary. It is expected that all cloud service providers will strive for certification on level 'high', because cloud providers are often part of the supply chain for sectors like government and vital infrastructures and services. In addition, certification can become mandatory. For example, the NIS2 Directive[4] is likely to facilitate this for cloud service providers that are in the scope of the NIS Directive[5]. Therefore, the proposed requirements on sovereignty in the Cloud scheme could have wide-ranging effects for companies (sub-contractors) involved in cloud service deliveries and their ability to develop their services and compete on the global market. This highlights the need for extensive impact analyses before including data sovereignty requirements in the Cloud scheme.

---

[1] The European Union Agency for Cybersecurity.
[2] Small and medium-sized enterprises.
[3] A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident (Cybersecurity Act, Article 52 under 1).
[4] Revision of the EU Network and Information Security directive, Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final).
[5] Network and Information Security directive, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

In addition, the sovereignty requirements appear to be difficult to implement and audit, and therefore will lead to high costs for the cloud service providers. The consequence will be that a significant number of cloud service providers might not be able to meet these requirements or at least will have a less competitive market position worldwide. This will hamper the competition in the European market for cloud service providers and restrict digital innovation.

We believe these concerns of the cloud service providers should be heard and addressed. In addition, we are concerned that the proposed sovereignty requirements in the Cloud scheme could have far-reaching implications for the European digital economy, as the digital economy and online services are based on one or more cloud services (including chains with subcontractors). We therefore emphasize that solid political guidance is required, including thorough analysis of potential consequences as well as careful assessment on what would be the appropriate legal framework.

2. Decisions on sovereignty require political guidance

The recent years have amplified the importance of enhancing trust in the global data economy and in international data flows. In general terms, we agree on the principle of strengthening Europe's data sovereignty in the context of EU's data strategy and the development of data spaces – all of which requires secure and well-considered solutions suited to fostering the new data economy of the European Union. The question what this means exactly, and how to achieve this, requires fundamental discussion at policy and even political level. We therefore propose that this topic will be put on the agenda of the Council. We should look at the whole framework and possible policy options, so that Europe's data sovereignty could be strengthened by enhancing control on European data by more generic, horizontal legislation at EU level instead of a specific certification scheme under the Cybersecurity Act.

3. Guiding principles for the way forward

Regarding any further development of the Cloud certification scheme we are proposing the following guiding principles:

a) The Cloud scheme must not be delayed more than it already is, in order for the implementation of the Cybersecurity Act to maintain momentum.
b) We should look at the whole framework of possible EU action, and see what measures could improve Europe's data sovereignty. For example, it could be strengthened by enhancing control on European data by more generic legislation at EU level such as the Data Act, rather than imposing technical security requirements in a cloud scheme under the Cybersecurity Act.
c) In specific circumstances (e.g. in the area of national security[6]) localization requirements can be justified. Such requirements should be supported by solid safeguards. This is in accordance with the Cybersecurity Act and the division of competences between the EU and its Member States.
d) The consequences of proposed sovereignty requirements should be studied carefully by relevant experts, including from competent authorities and relevant private sector stakeholders. An impact assessment of the requirements is needed and should include the economic effects.
e) The Cloud certification scheme concerns all categories of data, including both personal and non-personal data. Personal data is explicitly regulated by the GDPR[7]. Non-compliance of privacy issues (Schrems II judgement[7]), must be governed in the context of the GDPR. It is therefore advised to discuss this with the EDPB[8], instead of integrating this in the Cloud certification scheme.
f) Any possible measure should strengthen the European digital single market. We should not adopt measures which will hamper the single market or the development of SME's or startups. Fragmentation of the European market must be prevented.
g) Any possible measures should not breach existing or hamper future (bilateral, plurilateral or multilateral) trade-agreements between the EU and third countries.

[6] To be defined more specifically.

[7] General Data Protection Regulation, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. [7] Judgement of the Court of Justice of the European Union of 16 July 2020, Case C-311/18.

[8] European Data Protection Board.