B9+ joint statement[1]

EU Policy Makers must ensure that Cybersecurity Certification Schemes safeguard trust, resilience, free trade, and harmonisation of accessible, fair, and workable rules in the Internal Market.

June 20, 2023

Context

1. **The EU and its Member States have committed to leading this digital decade[2]. Business shares this ambition**. This means that Europe, in partnership with business and working with likeminded international partners, must intensify further trust and investment in secure, beneficial digital connectivity, innovation, inclusion, and adoption across the EU.
2. **European cybersecurity certification schemes developed under the Cyber Security Act (CSA) are important for the business community at large**, delivering the shared ambition for an increased security of digital products, services, and systems. Business supports a cybersecurity certification framework that achieves voluntary, robust, industry-relevant, state of the art, future proof and affordable schemes[3] without creating trade barriers or considerable adverse impact on European SMEs. In addition, a European Cloud Certification Scheme (EUCS) is essential for smooth provision and uptake of cloud service provision across the Internal Market.
3. **European business support an approach** that encourages digital capacities across the EU while remaining open to further international co-operation and trade with likeminded partners so Europe can access and safeguard the economic benefits of further digital transformation.[4]
4. In this context, **the development of a proposed *European Cybersecurity Certification Scheme for Cloud Services* (EUCS), in accordance with Article 54[5] of the Cyber Security Act must ensure the free movement of cloud services across Europe**. It must also ensure that certification levels are accessible and achievable for all market participants, creating high quality and level regulatory playing field. It should avoid disproportionate requirements that do not meaningfully add to cybersecurity or resilience.

---

[1] The B9+ Group is composed of the business confederations of the 12 digitally advanced (D9+) Member States: CEOE (Spain), VBO-FEB (Belgium), SPCR (Czech Republic), DI (Denmark), EE (Estonia), EK (Finland), Ibec (Ireland), FEDIL (Luxembourg), VNO-NCW (Netherlands), LEWIATAN (Poland), CIP (Portugal) and Confederation of Swedish Enterprise (Sweden).

[2] See https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en. Some of the objectives are to enable 75% of EU companies to use Cloud and enable 100% of key public services to be provided online by 2030.

[3] https://www.businesseurope.eu/publications/proposal-cybersecurity-act-businesseurope-position-paper

[4] Business Europe (2020) Smart technological sovereignty: how it could support EU competitiveness, B9+ Joint Statements (September, December, 2022 and May, 2023).

[5] Security objectives of European cybersecurity certification schemes

Concerns

While supporting cybersecurity certification, Business has the following concerns in relation to the proposed EUCS[6]:

1. **The conflation of political and technical issues in the proposed scheme.** Concerns remain that the proposed EUCS may not only contain technical requirements but genuine political issues, in particular proposals for EU data localization, HQ establishment and immunity from foreign legal requirements. Such political issues should be discussed and decided at the political level before being considered in a certification scheme. A certification scheme, however, is not an appropriate instrument to decide political questions[7].**The scope of the proposed scheme remains uncertain**. It is understood that the proposed scope for sovereignty criteria (which we understand are known as Independence from Non-EU Laws and recently as Protection of European Data against Unlawful Access) is intended for "*the most sensitive uses of cloud services*". However, there is a concern that a suggested categorisation of data use cases (data of particular sensitivity) will be open to broad interpretation that expands far beyond national security and classified information into a wide range of economic, public service and even commercial contexts[8]. A broad scope for interpretation would inadvertently lead to fragmentation of the internal market, impacting trust in further investment needed for 2030 ambitions. **The impacts of the proposed scheme remain uncertain**. An impact assessment is needed to get a clear picture of the market implications (such as possible hinderance of innovation and growth; competition issues; operational, administrative and practical implications, for example what are the implications for Cloud supply, for resilience or of potentially asking business to disregard non-EU legislative requirements). The fact that the scheme may be of a voluntary nature, does not exclude the necessity for a political decision regarding the possible geopolitical implications nor exclude the necessity for an impact assessment of the implications for the EU internal market also keeping in mind that the European Commission can through delegated (or implementing) acts mandate such certification schemes, same as a member State.

Call to action

EU legislators and National Cybersecurity Coordination Centres[9] should:

1. **Consider and agree political issues politically, not at a technical level**. Political considerations should not be delegated as per the ECJ ruling. Furthermore, schemes under CSA must be coherent and not contradict each other, and at the same time ensure consistency with other EU legislative initiatives e.g., DORA[10], Cyber Resilience Act, AI Act and others.
2. **Further engage industry, identify, understand, and address potential impacts**.

---

[6] Based on recent media reports (Reuters, Euractiv) and a leaked document in Politico, we understand that a new draft of the EUCS was recently shared with Member States. A proposed Annex J in the leaked document is a particular concern for business.

[7] The European Court of Justice states regarding delegation of powers (Case C 355/10) that “provisions which, in order to be adopted, require political choices falling within the responsibilities of the European Union legislature cannot be delegated”.

[8] It is understood the latest scope of Evaluation level 4 and definition of data of particular sensitivity also includes public health, public order, intellectual property, trade secrets and data necessary for maintenance of the State function.

[9] https://cybersecurity-centre.europa.eu/nccs_en

[10] For example, Recital 82 does not impose a data localisation obligation.

a. Sharing the latest draft scheme with the SCCG and an outline of the main proposed changes would allow for a broader and meaningful consultation process. A joint industry paper on enhancing the functioning of the SCCG was presented in November 2022.
b. Ensure the impacts of all proposed requirements in the draft EUCS scheme on businesses and the Single Market are thoroughly considered and addressed. Following the European Commission's Better Regulation Guidelines and Toolbox[11] regarding impact assessments for delegated and implementing acts, would facilitate a comprehensive understanding of the implications of a particular scheme and - based on this understanding - an informed choice of the potential technical requirements to be included.

3. **Ensure the scheme fosters coherence with other EU rules and international commitments and safeguards an approach** that encourages digital capacities across the EU while remaining open to further international co-operation and trade with likeminded partners so Europe can access and safeguard the economic benefits of further digital transformation.

[11] https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_en