BUSINESSEUROPE

STATEMENT

28/06/2022

# EU policy makers should ensure that Cybersecurity Certification Schemes promote trust, legal certainty, harmonisation of fair, workable rules, and free trade in the Internal Market

## CONTEXT

Over the recent years, the number and complexity of cyberattacks, cyber espionage and cyber sabotage has increased. Such attacks are directed at businesses, politicians, institutions, and citizens. In this regard, the Cybersecurity Act (CSA) is a key piece of legislation for the Digital Single Market which cannot reap its full economic and societal benefits if the technologies and services it consists of are not secure.

**BusinessEurope supports 'smart technological sovereignty'[1] approach.** It means the creation of a level playing field and an attractive business environment, where all companies can thrive and compete globally, while remaining open to further international co-operation and trade, so that Europe can access and safeguard the economic benefits of further digital transformation.

In this regard, **BusinessEurope believes that European cybersecurity certification schemes developed under the CSA** are crucial elements for the business community at large, delivering the ambition for an increased security of digital products, services, and systems. These schemes **must be specific, voluntary, industry-relevant, and affordable**[2].

With the increased pace of digitalisation of industry and public services, **the European Cloud Certification Scheme (EUCS) would become an important tool for clarifying the security level of cloud services and a cornerstone for cloud service provision in the Internal Market**, especially if the European Commission (Article 56, CSA) assesses that a specific scheme should be made mandatory. This prospect makes the meaningful, open and transparent engagement of stakeholders (Article 49(3), CSA) even more crucial.

## KEY CONCERNS

A consultation process on Cybersecurity Certifications Schemes that includes a broader and more regular dialogue with stakeholders

[1] Smart technological sovereignty: how it could support EU competitiveness – a BusinessEurope position paper

[2] The proposal for a Cybersecurity Act - a BusinessEurope position paper

BusinessEurope acknowledges the efforts made by ENISA during the preparation of the candidate scheme through the constitution of a Stakeholders Cybersecurity Certification Group and running a public consultation on the EUCS draft scheme in early 2021. We note however that going forward with the preparation of this and other certification schemes more can be done to **improve the transparency and enable an open dialogue**.

Cybersecurity certification schemes that promote harmonised requirements that fall within the defined responsibilities of ENISA

The cybersecurity certification **schemes should include technical requirements correlated to existing European regulations and legal requirements**. Recent information provided at ENISA's Certification conference in June 2022 however points to the inclusion of a political requirement for digital sovereignty in the draft EUCS although the notion of "sovereignty" is not yet defined at a European level.

BusinessEurope reminds the European Cybersecurity Certification Group, the Commission and the Council that in the basic legal act - the CSA - there is no such criterion defined. Furthermore, the European Court of Justice states with regard to 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".**

## CALL FOR ACTION

**BusinessEurope calls for a better involvement of all relevant actors from the impacted sectors in order to provide timely and informed opinion on the EUCS scheme**:

- A publication of the draft schemes on a quarterly basis and an outline of the main changes would allow for a broader and meaningful consultation process.
- Impact assessments of such schemes (especially if they take the shape of implementing act later) on the Internal Market and the free movement of services, following the European Commission's Better Regulation Guidelines and Toolbox (3 November 2021) with regard to impact assessments for delegated and implementing acts, would also 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.

**BusinessEurope calls on EU legislators to ensure the impacts of all proposed requirements** in the draft EUCS scheme on businesses and the Single Market are thoroughly considered and addressed. 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. NIS2; DORA; upcoming Cyber Resilience Act, etc).