

ECIS' comments on the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy

The European Committee on Interoperable Systems ("**ECIS**") commends the European Commission (the "**Commission**") for inviting stakeholders to provide their input on the regulatory environment for platforms, online intermediaries, data and cloud computing, and the collaborative economy.

ECIS has however identified a number of difficulties associated with responding to the current consultation. First, certain questions are phrased in a biased way, which would lead to misleading responses. Second, stakeholders are not able to provide comments in response to all the questions listed in the consultation, which makes answers to some of the "yes" or "no" questions misleading.

Below we set out some more specific comments in relation to certain sections of the public consultation.

On the role of online platforms

ECIS finds the definition of online platforms recommended by the European Commission as broad and vague given that it covers a very wide range of companies and activities. The breadth of scope and definition as could be read to include both B2C and B2B companies, both SMEs and multinational market players, and European and non-European companies. There are very different issues between B2B players and those with public, consumer-facing platforms. Most of the platform considerations addressed in the consultation are appropriate to the more public consumer-facing platform solutions; inclusion of B2B platforms may result in unintended consequences and needless constraints or burdens on such B2B services. It should also be noted that not all public, consumer-facing platforms provide the same type of service or face the same challenges. The nature of the consultation should endeavour to better recognise the variety of types of consumer-facing services offered and contexts of application to avoid, where possible, needless burdens or unintended consequences on those services.

The problems associated with online platforms that the European Commission aims to address are unclear. ECIS considers it is crucial for the European Commission to set out its objectives as clearly as possible in order for stakeholders to be in a position to comment on a definition of online platforms.

Online platforms in general refer to a business model, rather than an industry sector. For that reason, we consider that the European Commission should not use its proposed definition as a basis for any regulation.

On the need to regulate online platforms and the ability to move from one platform to another

ECIS is of the strong view that the perception that certain platforms have accumulated excessive power in the marketplace **should not** be addressed via the adoption of further regulation. This is especially the case in view of the benefits associated with the development and use of online platforms as described by the European Commission. Online platforms offer great opportunities for smaller and larger businesses to operate through them. Moreover, consumers are able to make more informed choices, and have access to a wider variety of products and services through online platforms.

We would encourage the European Commission first carefully to consider and make use of the already existing rules including the existing EU competition rules, as well as the current and future EU data protection framework before embarking in an endeavour to develop new regulatory measures. If the European Commission identifies market distortions and establish that healthy competition is threatened, it can apply EU competition rules to address any potential shortcomings.

On data location restrictions

ECIS considers data location restrictions justified under the guise of overly broad national or public security reasons as potentially damaging. They have the potential to impede free flow of data, and raise barriers to the industry to engage in international trade. Restricting free flow of data and imposing data location requirements can cause problems to both local and international providers. Local companies may not be able to access key technology services, which would limit their access to global markets, and their ability to offer their services worldwide, and therefore their potential to grow.

Furthermore, imposing data location requirements provides cover and legitimacy to other countries and regimes seeking to assert greater control over their populations under the guise of national or public security.

On the other hand, cybersecurity is not enhanced by imposing data location restrictions, especially because such restrictions can limit access to the most advanced security technologies.

All in all, any cybersecurity policies should strike the right balance between achieving national and public security, and supporting both SMEs and bigger enterprises to grow globally and enjoy the benefits of technology innovation and informatisation.

On the European Cloud Initiative

First, with respect to cloud service providers' transparency concerning the security and protection of users' data, ECIS notes that the data protection and security objectives and principles that were set out in the "Data Privacy Code of Conduct" group adopted by the industry led Cloud SIG should be adhered to by cloud service providers. The Code of Conduct follows Directive 95/46 on data protection and the ISO 27000 set of standards.

Second, with respect to the existing contractual practices, ECIS is of the view that those practices provide a fair and balanced legal and technical framework for cloud service providers. Contracts are designed to fit specific user requirements, but also aim to maintain the time of negotiations and legal costs to a minimum.