CISPE Response to the public consultation on Digital Services Act

About CISPE

Cloud Infrastructure Services Providers in Europe (CISPE.cloud) is a non-profit association that focuses on developing greater understanding and promoting the use of cloud infrastructure services in Europe. Members based in 14 EU Member States range from SMEs to large multinationals. CISPE members invest billions of euros in Europe's digital infrastructure and currently provide services to millions of customers, including organisations in multiple countries and locations outside the EU.

Security and data protection are cornerstones of the CISPE constitution. It was the first association in the EU to develop a dedicated GDPR-compliant Code of Conduct for Data Protection for the sector, aligning with strict GDPR requirements to help providers comply while bringing clarity to customers to help them select providers and build trust in their services.

CISPE has always aligned with EU values: since 2016 all services declared under the CISPE GDPR Code of Conduct offer customers the ability to opt for services that securely store and process data exclusively within the EEA. CISPE also co-chaired the cloud industry working group (European Commission) to develop codes of conduct for reversibility and data portability under the Regulation on the free flow of non-personal data.

1. Introduction: the DSA presents a unique opportunity for the Commission

Cloud Infrastructure Services Providers in Europe (CISPE) envisage a prosperous and innovative European Union with a vibrant Digital Single Market that delivers robust economic growth for Europe and benefits all European citizens. The technology to deliver this vision is already here: cloud computing.

Cloud is the catalyst for genuine digital and environmental transformation.

Cloud infrastructure services provide the underlying IT infrastructure tools for organizations and individuals to set up processing, storage, networks and other fundamental computing resources to deploy and run software and systems themselves. These include operating systems, applications, websites and streaming content, artificial intelligence, connected devices, autonomous vehicles, smart factories, Internet of Things and the next generation of cellular connectivity: 5G services.

These cloud services make it possible for businesses and governments to build their own systems and deliver essential services to billions of citizens and consumers, reducing costs and reducing wasted or underutilised resources. Cloud accelerates the pace of innovation, giving even the smallest companies in the EU access to vast virtual resources in minutes, anywhere in the world. To build on this technology and enable a robust Digital Single Market, Europe requires an environment that fosters and protects continuous innovation, particularly for SMEs.

CISPE encourages the Commission to take the opportunity presented by the DSA to enact policies that recognise the growing importance and unique characteristics of cloud infrastructure services to allow the European cloud infrastructure industry to flourish. The two most important opportunities in the DSA are:

1. For the Commission to create the first ever definition of "cloud infrastructure services" that should benefit from a "safe harbour" due to its unique characteristics.
2. To address the anticompetitive practices of entrenched software providers that hamper European innovation, unnecessarily increase costs, reduce consumer choice and inhibit the availability of cloud computing to European citizens.

2. Cloud infrastructure services are content agnostic without control over or knowledge of end user content

Cloud customers or their third-party end-users (e.g. social networks, software vendors) decide how to use these cloud infrastructure services when building their applications, environments or websites, maintaining control over their own content and IT environment. Cloud infrastructure services support a virtually unlimited number of use cases, determined by customers. Customers (not cloud infrastructure providers) control what content is uploaded, how that content is made available to the public, and to whom it is made available. For example, customers may choose to encrypt information that is not intended for the public; cloud infrastructure service providers do not make such decisions.

Indeed, it is fundamental to cloud infrastructure services that providers do not access or use customers' data other than in an extremely limited manner as necessary to maintain or provide such services.

Customers including those with high IP protection considerations, such as aircraft manufacturers, automakers and energy companies, demand that cloud infrastructure providers cannot access or conduct monitoring or surveillance of their content. Furthermore, to require this is incompatible with the services' role of providing underlying internet tools as well as being incompatible with fundamental freedoms relating to the right to privacy. This important principle allows privacy requirements and expectations to be met, protects customers' trust in the cloud and users' trust in the internet itself, and places the responsibility for monitoring of conduct and content where it belongs: with the cloud infrastructure services customer.

In a cloud infrastructure services context, the responsibility for security is shared, based on the degree of control over the data. Service providers are responsible for ensuring the cloud itself is secure while cloud customers are responsible for securing their own content and data, including building secure applications and environments. This separation of responsibilities distinguishes cloud infrastructure from other types of cloud services and other types of digital services, like social media. Cloud infrastructure service providers should not be confused with other providers who offer services via the internet or online content sharing providers.

CISPE urges the Commission to ensure that any rules on responsibility take into account important differences between cloud infrastructure services, which do not have visibility of or control over content, and other services offered on the cloud that do, such as online content sharing providers.

3. Technical impracticability in taking down specific pieces of content

Given the nature of how cloud infrastructure services work, it is technically impracticable for a cloud infrastructure provider to identify the location of specific pieces of customer content stored on its services.

To comply with a request to take down or disable access to a piece of content (e.g. a photograph) uploaded onto an online platform that is run on cloud infrastructure services, a cloud infrastructure provider likely has little choice but to shut down or disable access to a large portion of customer content from other users of that platform. This could include removing access to an entire website (e.g. a newspaper), closing down access to lawful content, related services and potentially a large number of other users, or even shutting down services to other customers. Over-disabling or removal of content, including legitimate content, is an inevitable consequence of content moderation requirements when imposed on cloud infrastructure providers.

Any measures to disable or remove online content should be proportionate to the threat, specifically target the illegal content in question and avoid indiscriminate disabling or removal of legitimate and legal customer content.

CISPE urges the Commission to refrain from extending content moderation obligations to cloud infrastructure providers, given the technical impracticability of taking down specific pieces of content, and the significant risk of disruption of service to legitimate cloud customers or their third-party end-users.

4. Introduce a future-proof definition of cloud infrastructure services including "safe harbour"

The safe harbours in the E-Commerce Directive (ECD) have been essential to the development of an innovative digital economy in Europe and the protection of fundamental freedoms, such as freedom of expression and respect of user privacy. The principle that certain digital services cannot be held liable for their users' wrongdoing as long as they act expeditiously when they have actual knowledge of specific infringements achieves the right balance of protecting those rights whilst allowing timely and proportionate actions against illegal content and activities.

CISPE firmly believes the categories of "mere conduits", "caching services" and "hosting services" remain valid for protecting today's digital intermediary services that fall within these categories.

We also believe it is appropriate to create a fourth category for "cloud infrastructure services" to clearly establish appropriate safe harbour protections for these services. This is necessary given the unique characteristics of cloud infrastructure services in having no control or knowledge of customer content on their systems, and in being processors rather than controllers of customer data. The new safe harbour for cloud infrastructure services should refer to "cloud infrastructure services" (which should be a new defined term in the DSA) and should be consistent with the existing hosting services safe harbour in the ECD. Creating a separately defined category will ensure these services can continue to benefit from the safe harbour and ensure they are appropriately distinguishable in current or future legislation, such as the Terrorist Content Online Regulation (TCO), which references the broader definition of "hosting service provider" from the ECD. In the TCO, the definition of "hosting service provider" created confusion by potentially capturing cloud infrastructure services, necessitating a clarification elsewhere in the draft.

In summary, the DSA should complement and provide greater clarity to the fundamental principles of the ECD and make clear the roles and responsibilities of different actors online. An important way it can build on the ECD is to introduce a definition of "cloud infrastructure services" that accurately captures its unique characteristics, and introduce a new safe harbour for cloud infrastructure services to further the development of Europe's digital economy in Europe and protect fundamental freedoms.

CISPE experts stand ready to work with the Commission to help create the first definition of cloud infrastructure services in Europe, which will benefit from a safe harbour (see also point #2 above).

5. General monitoring and filtering obligations should not be imposed on cloud infrastructure services

CISPE believes the prohibition against general monitoring obligations contained in the E-Commerce Directive remains appropriately scoped and plays an important role in protecting fundamental freedoms (notably the right to privacy) as well as start-up businesses in Europe and all digital service users.

A fundamental characteristic of cloud infrastructure services is that providers do not access or use customers' data other than as necessary to maintain or provide the services. This gives customers, including individuals, businesses and governmental agencies, confidence that their data remains private, secure and protected from unauthorized disclosure or surveillance. This important limitation means cloud infrastructure services providers do not have the ability to use filtering technology such as "hashtag recognition" to monitor content. The technical reality is that cloud infrastructure providers do not have access to review content, encrypted or otherwise, and are not aware of the purpose of the content that end users may have (see CISPE Data Protection Code of Conduct).

This is in stark contrast to online content or file sharing and social media applications or platforms that do have access to individual content and control rights, down to the most granular piece of content on their platform. That is, those providers are able to view and take down or delete a specific individual piece of content made available to the public or target an individual end user. Lumping cloud infrastructure in with these services would have consequences in a field where Europe is seeking to assert its strategic autonomy.

In terms of that strategic autonomy, Cloud infrastructure services are enabling 5G and IoT connected cars and objects. Imposing monitoring requirements and the use of monitoring software tools on the infrastructure layer could have a seriously adverse effect on the functioning of these new IoT products or services and create new "back door" security vulnerabilities. This could undermine the EU strategic autonomy in these sectors.

We therefore believe the DSA should not allow Member States to impose a general obligation on cloud infrastructure service providers to monitor the information that users transmit or store. This would also apply to any obligations to prevent the re-upload of content (stay-down obligations) since this would require monitoring of uploaded content.

CISPE is asking the Commission to agree to uphold the limited liability principles in the DSA for cloud infrastructure services, and that a general obligation to monitor content should not apply to such services.

6. Address software licensing abuses

CISPE fully supports a strong EU internal market, enabling the creation, growth and successes of its digital and non-digital cloud computing customers—with promoting and protecting consumer welfare at its heart.

For CISPE, there is no separate "digital economy" that can be defined with any degree of accuracy and distinguished from the rest of the economy. The recent COVID-19 crisis demonstrates how critical cloud computing is not only to the functioning of the economy at large but also to social and working life, education and even the administration of justice.

New regulation, to the extent it is required at all, should apply equally to online and offline business models. Limiting regulation to digital business models risks distorting competitive dynamics, thus hampering innovation and growth, and harming consumer welfare to the detriment of businesses and consumers. New rules should aim to promote long-term consumer welfare and address the malfunctioning of markets that are critical to Europe's digital agenda and have not been fixed by traditional competition law.

CISPE is therefore urging the Commission to consider using the DSA as a way to tackle a decades-old problem that affects the healthy functioning and constitution of the market for cloud computing services in Europe.

Our top priority is serving cloud infrastructure users in Europe. In contrast, some major software suppliers aggressively use their licensing terms to give themselves an unfair competitive advantage over other cloud providers regardless of the impact on cloud consumers.[1] Specifically: the use of bundles, subscription services with auto-upgrade terms, elimination of Bring Your Own License (BYOL) rights, plus significant price hikes and restrictions on running their software on cloud infrastructure provider platforms other than their own are significantly reducing consumer choice while simultaneously increasing costs.

As newer entrants in the IT services segment, CISPE members have are disrupting an industry that has been dominated by large software vendors for decades. To protect and entrench their positions now and in the future, these legacy software vendors are using their position to reduce competition in cloud infrastructure services. This is an abuse of true gatekeeper power and needs to be addressed.

CISPE is an active member of the SWIPO (Switching and Porting) initiative that has been developing under the auspice of the Commission to make the Article 6 (Data Porting) of the Free Flow of non-personal Data Regulation (FFoD) a reality. If the ongoing malpractices are tolerated, this would seriously undermine the objectives of the free flow regulation and the SWIPO initiative.

CISPE urges the Commission to help end the abusive practices by major software suppliers, imported from an on-premises IT environment. The smooth adoption of cloud computing in Europe and the larger development of Europe's digital and online ecosystems are at stake.

[1] For example: the July 2020 complaint made to the Commission by Slack regarding Microsoft's practices of tying its Teams product to the company's dominant productivity software products e.g. https://www.cnbc.com/2020/07/22/slack-accuses-microsoft-of-anticompetitive-practices-in-eu-complaint.html