

**Leaseweb Global B.V.****formal submission to the Digital Services Act Consultation Package 7 September 2020****1. Introduction**

With this letter Leaseweb Global B.V ('**Leaseweb**') with its global headquarters in Amsterdam, The Netherlands, formally participates in the Consultation on the Digital Services Act package. Leaseweb is a member of the Cloud Infrastructure Services Providers in Europe (CISPE).

Leaseweb is a leading Infrastructure as a Service (IaaS) provider serving a worldwide portfolio of 18,000 customers ranging from SMBs to Enterprises. Services include Public Cloud, Private Cloud, Dedicated Servers, Colocation, Content Delivery Network, and Cyber Security Services supported by exceptional customer service and technical support.

With more than 80,000 servers, Leaseweb has provided infrastructure for mission-critical websites, internet applications, email servers, security, and storage services since 1997 when Leaseweb was founded by its Dutch shareholders. Still today, Leaseweb is fully owned by its founders, headed by its Global CEO in the Netherlands.

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.

The company operates through its globally and independent organized Leaseweb Sales Companies 20 data centers in locations across Europe, Asia, Australia, and North America , all of which are backed by a superior worldwide network with a total capacity of more than 10 Tbps, with its global footprint the EU based principles are clearly leading.

Leaseweb is a diversified hosting service provider in its role as online intermediary, with a focus on the professional market. Leaseweb offers the 'building blocks' for hosting infrastructure to its B2B customers. The scope of the services provided by Leaseweb is limited, in the sense that Leaseweb does not provide SaaS-services or equivalent software or any content services. Leaseweb for example does not manage, access or control end user applications and content. Nor does Leaseweb:

- (a) provide content or content services to its customers; or
- (b) actively monitor the way its services are used by a customer or an end user; or
- (c) verify or have the option to verify what content is available or stored on the servers used by its customers.
- Leaseweb sets out the policies for the use of Leaseweb's Services in the "Leaseweb Policies", such as the Acceptable Use Policy and Abuse Compliance Policy. For the latest version of the Policies, please visit our website at: <https://www.leaseweb.com/legal/sales-contract>. For third party abuse



notifiers the following link provides for abuse notifications as part of the Leaseweb Notice and Take Down Procedures.

The growth of online activity has given rise to cybercrime, which poses new challenges for law enforcement authorities to deal with crime on the internet. This results in the need for law enforcement to perform investigations in the digital realm using their local powers subject to the specific jurisdictions. The reason that law enforcement authorities reach out to hosting companies like Leaseweb can be understood by the tracking and tracing of the involved IP address of the suspect. The hosting company could possibly disclose (under valid orders required by law) the details behind the specific IP address and can follow up to the third party content provider for passing on abuse notifications from third party abuse notifiers.

Leaseweb Sales Companies take any Law enforcement orders and abuse notifications serious and each request is carefully reviewed by Leaseweb's Compliance team. Incomplete, unclear, or unauthorized requests are rejected. Only complete, valid requests authorized by the correct judicial authority of the respective jurisdiction of that Leaseweb Sales Company are processed.

Instead of providing for statistics and absolute numbers to the extent permitted by local law (like in some other transparency reports of content platforms) Leaseweb is transparent in its position as IAAS unmanaged cloud hosting provider (no content platform) towards law enforcement authorities.

Leaseweb's memberships and alliances with hosting organizations (DHPA, DINL and EU based CISPE), facilitate Leaseweb in preparing for the new regulatory framework and topics, now being discussed.

As a result, Leaseweb keeps a close eye on the development of new regulations within our IAAS and hosting industry including this Digital Services Act Consultation Package to ensure ongoing compliance and realistic efficient approach for current and future regulations.

2. Cloud Infrastructure Services

Cloud infrastructure services like Leaseweb are located deep in the internet stack. We provide the underlying IT infrastructure tools for organizations to set up processing, storage, networks and other fundamental computing resources to deploy and run software and systems themselves.

Cloud users (e.g. SAAS, PAAS, social networks, software vendors) decide how to use these cloud infrastructure services when building their applications, environments or websites, and these third parties maintain control over their own content and IT environment. Such cloud users control what content is uploaded, and themselves may choose to encrypt information. Third party customers including those with high IP protection considerations, demand that cloud infrastructure providers cannot access or to conduct monitoring or



surveillance of their content. Also, security is separated and distinct for IAAS online intermediaries: service hosting providers are responsible for ensuring the cloud itself is secure, while cloud users and their customers are responsible for building secure applications and environments.

Cloud infrastructure (IAAS) services are content agnostic and do not have control over or knowledge of third party customer or end-user content. Therefore, Leaseweb urges the European Commission to ensure that any regulations take into account important differences between cloud infrastructure services, which do not have visibility of or control over content, and other digital services offered on the cloud which build upon our infrastructure.

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 remove a piece of content (e.g. a photograph) uploaded onto an online platform that is run on cloud infrastructure services, a cloud infrastructure provider cannot remove it and will pass on the request to the content provider. Leaseweb as online intermediary can only in many cases and dependent on the users IP address disable access to a large portion of customer content from other users of that platform. This could include disable 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 third party end user services in the network. Over-removal of content including legitimate content causing legal liability towards third parties harmed without cause is an inevitable consequence of content moderation requirements when imposed on cloud infrastructure providers.

3. General Monitoring and Filtering Obligations continued as not applicable

Leaseweb 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 third party user's data other than as necessary to maintain or provide the services. This gives third party 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. 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.

We therefore believe the Digital Services Act 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.

4. Safe Harbour

The safe harbours in the E-Commerce Directive (ECD) have been essential to the development of an innovative digital economy. 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.

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

As stated above and aligned with our role as online intermediary, as an IaaS hosting provider, we do not have access to the content on the network services and therefore depend on external feeds and abuse notifications from third parties to become aware of any internet misuse taking place in the Leaseweb network.

Any measures to remove online content should be proportionate to the threat, meaning actions must specifically target the illegal content in question and avoid indiscriminate removal of legitimate content.

In order to act expeditiously, all Leaseweb Sales Companies adhere to strict internal Compliance policies that are aligned with the requirements of local laws and are applied globally. As good hoster, Leaseweb applies these strict Compliance Policies to achieve our high Compliance Rate and short Uptime of notified abuse.

The Notice and Take Down process is part of the Leaseweb Policies to demonstrate Leaseweb's duty of care to comply with the applicable regulations as set above and includes the obligations Leaseweb is requiring from third parties, including its customers and the end-users of its customers, to properly execute the Notice and Take Down procedures under the Leaseweb Policies and applicable law such as the EU e-Commerce Directive article 14.



Leaseweb Sales Companies - as a responsible good hosting provider - require having every abuse notification resolved by the parties responsible for such content within (at most) 24-48 hours whereby this deadline is included in the abuse notification to such responsible content providers. In some specific cases a faster resolution time is fiercely demanded by Leaseweb based on its Policies. For example, Leaseweb applies the strict timeline of only one (1) hour for CSEM ('Child Sexual Exploitation Material') abuse notifications, as a maximum Uptime, leading to disabling the services in case the abuse notification has not been properly resolved.

4. Regulatory focus: IAAS hosting provider as online intermediary clearly recognized

We also believe it is appropriate to create a fourth category for "cloud infrastructure services" to clearly establish appropriate safe harbour protections for these digital network 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 formal processors rather than controllers of customer data*.

Creating a separately defined category will ensure these services can continue under the regulatory proportionate regime of safe harbour and ensure they are appropriately distinguishable from current and/or future legislation, such as the Regulation for Terrorist Content Online (TCO) that generally references the broader definition of "hosting service provider" in the ECD.

In the TCO, the definition of "hosting service provider" created acknowledged confusion by potentially capturing cloud infrastructure services, necessitating a clarification elsewhere in the regulation (draft).

In summary, the Digital Services Act should complement and provide greater clarity to the fundamental principles of the e-Commerce Directive and make clear the roles and responsibilities of different actors online. An important way it can build on the e-Commerce Directive 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.

Leaseweb urges the European 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 third party users and content providers.

Leaseweb is asking the European Commission to agree to upholding the limited liability principles in the Digital Services Act for cloud infrastructure service providers, and that a general obligation to monitor content should *not* apply to cloud infrastructure service providers.



[REDACTED]

EU-Transparency number: 614454339447_22

[REDACTED]

Amsterdam

7 September 2020

[REDACTED]

Leaseweb Global B.V.