LEASEWEB DSA TRANSPARENCY REPORT 2025

LEASEWEB DEUTSCHLAND GMBH
LEASEWEB NETHERLANDS B.V.

ISSUED BY THE LEASEWEB LEGAL DEPARTMENT
VERSION: 28 FEBRUARY 2026

Get in Touch

www.leaseweb.com info@leaseweb.com in/company/leaseweb f/leaseweb

TABLE OF CONTENTS

1.LEASEWEB DSA TRANSPARENCY REPORT 2025 **3**

2.Leaseweb Illegal Content Governance **5**

3.Leaseweb As Good Hoster **7**

3.1 Abuse Handling Process 8

3.2 Abuse Handling Of Cloudflare 8

4.Notices – Illegal Content – Notice and Take Down Process **10**

5.Law Enforcement And Member State Orders **13**

6.Regulatory Matters **14**

6.1 Leaseweb's Anti-Csem Policies 14

6.2 Offlimits Instant Image Identifier (3is) 14

To report an abuse notification with the Leaseweb Sales Entities, please visit: www.leaseweb.com/abuse-handling

For media/press contact, please visit: Leaseweb or send an email

1. Leaseweb DSA Transparency Report 2025

This Leaseweb DSA Transparency Report 2025 is published in relation to the requirements of the Regulation (EU) 2022/2065 Digital Services Act (hereafter "DSA"). It covers 1 January – 31 December 2025 reporting.
At the Leaseweb website https://www.leaseweb.com/en/about-us/legal/compliance-reports the Leaseweb DSA Transparency Report 2025 is listed based on the following DSA implementing regulations Annexes I and II: Brussels C(2024) 7005 final COMMISSION IMPLEMENTING REGULATION (EU) of 4.11.2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council in Annex I and the Instructions for filling in the transparency reports templates under Annex II.

The Leaseweb DSA Transparency Report covers the period from 1 January 2025 to 31 December 2025 and is herewith timely and duly provided and made publicly available by Leaseweb Netherlands B.V. (Netherlands, Leaseweb NL) and by Leaseweb Deutschland GmbH (Germany, Leaseweb DE), both acting separately as (unmanaged) Infrastructure as a Service Provider (IaaS). Each Leaseweb Sales Entity is subject to the EU DSA regulation in its capacity as an intermediary service provider and hosting service provider as per DSA Article 15.1. Annex I EU Templates Part. 1 include the Reporting Identification and Reporting Periods of Leaseweb.

Leaseweb has taken fair and reasonable orientation including taking part in the Internet & Jurisdiction Policy Network, Regulatory & Legal Track of the Internet Infrastructure Forum held in London (February 10-11, 2026) and such earlier meetings, to match and apply the templates concerning the transparency reporting obligations of providers of intermediary services under Regulation (EU) 2022/2065 of the European Parliament and of the Council and the Instructions for filling in the transparency reports templates per Annex.

The relevant Digital Service Providers (https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs) are the local authorities: ACM for Leaseweb Netherlands B.V. and the BNetzA for Leaseweb Deutschland GmbH.
Now, therefore, the transparency reporting obligations for providers of intermediary services of the Digital Services Act as set out in Article 15.1 DSA are listed hereunder with reference made to the specific Chapter in this Transparency Report, in addition to the (Annex I) EU Templates relevant to Leaseweb as filled in and uploaded at the Leaseweb website https://www.leaseweb.com/en/about-us/legal/compliance-reports:

EU Templates	Part. 1 (Identification-Reporting Period),
EU Template	Part. 3 (Member State Orders),
EU Template	Part. 4 (Notices, Trusted Flaggers), and
EU Template	Part. 7 (Appeals and Recidivism).

As per Article 15. 1 a) DSA listing the number of orders received from Member States authorities, is referred to in Chapter 5: Law Enforcement, whereby the related EU Templates Part. 3 (NL, DE) are filled in and uploaded.

As per Article 15.1 b) DSA listing the number of notices submitted in accordance with Article 16 DSA, categorized by the type of alleged illegal content concerned, including the number of notices submitted by Trusted Flaggers, is referred to in Chapter 4: Notices, Illegal Content, NTD whereby the related EU templates Part. 4 (NL, DE) are filled in and uploaded.

As per Article 15.1 c) DSA information on engagement in content moderation is provided by clarifications that content moderation is exempt to the unmanaged IaaS operating model like Leaseweb DE and Leaseweb NL- by means of descriptions of the abuse handling process, the compliance team organization, the availability, visibility and accessibility of such information provided to the recipients of the service (meaning customers) and the Notice and Take Down, the automated NTD tool, categorized by the type of illegal content or violation of the terms and conditions (Policies), and by the type of restriction, is referred to in Chapters 2, 3 and 4 whereby the related EU Templates Part. 5 (own initiative content moderation based on illegal content) and EU

1. Leaseweb DSA Transparency Report 2025

Templates Part. 6 (own initiative content moderation based on terms and conditions) (DE, NL) are exempt to unmanaged IaaS operating model.

As per Article 15.1 d) DSA listing the number of complaints received through the internal complaint-handling systems, is referred to in Chapter 2: Illegal Content Governance, whereby the related EU Template Part. 7 (appeals and recidivism as internal complaint) (DE, NL) is filled in and uploaded.

As per Article 15.1 e) DSA information of the Leaseweb automated tools for the abuse handling procedures with indicators of the accuracy and the possible rate of error of the automated means used and any safeguards applied, is referred to in Chapter 3: Good Hoster whereby the related EU Templates Part. 8 (for tool based content moderation as automated means) (DE, NL) are exempt to unmanaged IaaS operating model.

This Leaseweb DSA Transparency Report 2025 presents how Leaseweb, as an online intermediary/hosting provider (not as a platform), handles internet abuse and illegal content with care and diligence, whereas it is made clear that content moderation is not part of the Leaseweb IaaS operating model for abuse handling.

2. Leaseweb Illegal Content Governance

Leaseweb NL and Leaseweb DE are each leading Infrastructure as a Service (IaaS) hybrid providers offering services ("Services") ranging from Public Cloud, Private Cloud (Bare metal servers), Dedicated Servers, Colocation, Content Delivery Network, and Cyber Security Services supported by customer service and technical support, to be found at https://www.leaseweb.com/en/.

Leaseweb NL and Leaseweb DE operate each individually and separately with distinct management, each under local applicable law, whereby the EU-based standards, including GDPR, are leading policy by Leaseweb from its EU-based head office in the Netherlands, jointly referred to as "Leaseweb".

In this Leaseweb DSA Transparency Report 2025, Leaseweb explains the setup of the Compliance Department performing Member State Orders and Abuse Handling for incoming subpoenas, orders, instructions, and abuse notifications for Leaseweb NL and Leaseweb DE under their own local Policies subject to and applying the DSA, relating to criminal or civil law grounds to act.

The Leaseweb Compliance department has built up substantial experience and can be approached for providing in-depth knowledge on abuse handling processes. Also handling more complex and ethical categories of internet abuse and misuse that are causing public debates for its illegal content in need of combatting are supported by Leaseweb. In addition to the illegal content categories listed in the DSA Annex I EU Templates, Leaseweb refers to its customer binding Policies, including abuse handling and prohibited use of the Leaseweb Services. Leaseweb Policies also cover non-DSA categories like DDoS, Hack Gambling, Malware, Spam, and VoIP, duly taken care of for abuse handling by the Leaseweb Compliance department, not pre-categorized under the DSA Annex I EU Templates.

In addition, the Compliance department is trained for Customer Verification, ensuring a neutral evaluation of orders via the introduced KYC ('Know Your Customer') procedure to aim for a clean network and clean customer base, reducing risks of internet misuse.

As Leaseweb is structured in accordance with its sovereign entity split, each Leaseweb Sales Entity, including Leaseweb NL and Leaseweb DE, provides Services to its customers governed by its Sales Contract Schedules applicable to any Sales Order, including its Acceptable Use Compliance Policies. In the DSA, this is qualified and referred to as "terms and conditions", transparent and applicable. The "terms and conditions" are available at Leaseweb's website https://www.leaseweb.com/en/about-us/legal/sales-contract and can be read, downloaded, printed, and saved locally.

These Compliance Policies include customer requirements for a clean network, fair use of services, and compliance with law enforcement, subject to local applicable law where the Leaseweb Sales Entity is incorporated, and its services are located, operated, and provided. The Leaseweb Sales Entity Policies are applicable to all use of Services by a customer, also in case of trials, Proof of Concept, free-of-charge discounts, and any use of the network to avoid and combat abuse and illegal content while using the Leaseweb services. For the latest version of the Policies: https://www.leaseweb.com/legal/sales-contract.

Illegal Content Governance for Leaseweb NL and Leaseweb DE is established in the Compliance Department at the Leaseweb Headquarters in Amsterdam and supported by the Legal Department for regulatory guidance. The Compliance Department handles, subject to local law and subject to its Leaseweb Policies, all incoming abuse notifications and law enforcement requests, which can be easily reported by email and through a web form.

As set out above, Leaseweb's dedicated Compliance Department deals with copyright holders, copyright agencies, law firms, law enforcement authorities, foundations, so-called hotlines, Trusted Flaggers, and organizations focused on Abuse Handling and third parties who file abuse notifications.

Per Article 15.1 d) DSA listing the number of complaints received through the internal complaint-handling systems, is referred to in Chapter 2: Compliance Management above

2. Leaseweb Illegal Content Governance

amounts to whereby the related EU Template Part. 7 (appeals and recidivism as internal complaint) (DE, NL) is filled in and uploaded with zero (0). No complaints, disputes, legal court cases, or legal claims have been received by the Compliance Department complaint handling systems or any communication

3. Leaseweb as a Good Hoster

Leaseweb functions as an unmanaged Infrastructure as a Service (IaaS) cloud provider with a focus on the professional market. Leaseweb offers the 'building blocks' for hosting infrastructure to its B2B customers. Leaseweb does not provide SaaS services or equivalent software or content services. Leaseweb, for example, does not manage or control end-user applications and content. Nor can or 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.

Due to the size and quality of the network and sharp pricing, both Leaseweb NL and Leaseweb DE are cloud infrastructure providers for bandwidth-intensive, user-generated content sites, where users can share and contribute content.

Leaseweb as Good Hoster and, in its relationship with its customers, sets out the Policies for the use of Leaseweb's Services in the "Leaseweb Policies" (referred to as terms and conditions under the DSA), such as the Acceptable Use Policy and Abuse Compliance Policy https://www.leaseweb.com/legal/sales-contract.

As Good Hoster, Leaseweb provides that the Policies will be updated from time to time, not only to apply new applicable regulations but also to consider new Leaseweb compliance requirements. Such as the mandatory obligation for VPN Providers to keep their PTR records up to date, reflecting their business identification. At Leaseweb's request, a customer must provide their details to be visible in the IP registration. Also, upcoming E-Evidence requirements, the Terrorist Content Online and Digital Services Act regulations and requirements are included in the Policies to optimize a clean network and user compliance.

As an IaaS (hosting) provider, in principle, Leaseweb does not have access to the content of customers' services and therefore, depends on external feeds and abuse notifications from third parties to become aware of any internet misuse taking place in the Leaseweb network. This online intermediary position and the IaaS operating model for a hosting party are crucial for the reporting of illegal content. Per DSA, Leaseweb considers the rules for online intermediary and hosting service providers applicable, always considering the actions that are available to an IaaS provider to remedy abuse notifications for illegal content.
As Good Hoster, Leaseweb takes a proactive approach where possible to keep our clean network. We seek and reach out to foundations and organizations (so-called "Feeds") that combat online internet abuse and request or subscribe to the data that these Feeds make available for the purpose of combatting internet abuse. The Leaseweb Sales Entities receive input from a variety of Feeds such as Spamhaus, Shadow Server, OFFLIMITS, and others. Whenever a Feed is available, the Compliance team will investigate possibilities to subscribe to it or to receive the input in an alternative way. This helps combat spam and fraud.

As Good Hoster Leaseweb has invested, developed, and undertakes ongoing enhancements in its automated IaaS notification tool, the Abuse Handler. Feeds are imported, where possible, into the Abuse Handler, an in-house developed abuse handling system based on all the years of anti-abuse experience and knowledge, and are duly processed. By subscribing to such Feeds there is an expected increase in the number of abuse notifications to be received by Leaseweb. The above-mentioned combination of abuse Feeds and notifiers abuse notifications allows Leaseweb as Good Hoster to identify patterns of abusive behavior that Leaseweb aims to act upon, for example, bringing to light so-called "repeating offenders" which allows Leaseweb to take and anticipate appropriate actions.

Within the Leaseweb network, such Feeds also provide a better understanding and more insight into the health of the Leaseweb network, which is relevant for Leaseweb's Good Hoster and anti-abuse ambitions, in addition to Leaseweb's ambition for DSA compliance.

3. Leaseweb as a Good Hoster

It is important to note that the number of abuse notifications itself does not qualify a Good Hoster or a bad hoster: the larger the business and the larger the customer base, or some categories of services like VPN, the more such abuse notifications, even with all applicable Policies. Important to note for Leaseweb as Good Hoster is that the absolute number of abuse notifications or reported websites or domains is subjective, as it is fully dependent on the size of the network and the number of customers for the context of statistics.

However, Leaseweb applies its continuous improvement for a clean network in its role of IaaS (online intermediary) to the extent allowed by law and technically feasible (please note: no detection, pro-active measures, and no general monitoring is allowed, and Leaseweb Sales Entities function as cloud infrastructure providers, where by its customers are notified under Notice and Take Down actions).

What matters is how a hoster handles the abuse notifications it receives. For a Good Hoster, "Uptime" (i.e., the length of time reported content remains online and the speed with which it is resolved) is a key performance indicator (KPI) for Compliance and reflects Leaseweb's Good Hoster attitude.

Abuse handling process

In accordance with the DSA and all previous years of compliance operations under the previous E-Commerce Directive, the performance of the Notice and Take Down procedures starts with the third-party abuse notification, referred to as the "notice". The processing of these abuse notifications is in line with regulations and Leaseweb Policies under the Notice and Take Down procedures.

Notice may be submitted via Leaseweb's transparent, easy-to-find, and effective website, email, or web form. Many times, Notices are sent by letter. In case an abuse notifier has reason to send an abuse notification, any abuse email addresses of Leaseweb NL and Leaseweb DE are duly published on the Leaseweb website.

Leaseweb carefully explains to abuse notifiers to ensure that a valid Leaseweb Internet Protocol (IP) address is included in the abuse notification. This is required to successfully match the abuse notification with the account using the Leaseweb network. Without a valid Leaseweb IP address, the abuse notification cannot be matched, which will delay any further processing of such abuse notification. This is also in line with the DSA requirements.

Every abuse notification sent to Leaseweb NL or Leaseweb DE is processed by our state-of-the-art, in-house developed abuse handling tool. The Compliance team works with this abuse handling tool, deploying seasoned experience and know-how. The Abuse Handler processes notifications 24/7, 365 days a year for notifiers. Every received abuse notification is forwarded after evaluation of the content and keywords, resulting in a continuous and swift processing of abuse notifications.

The key words in the Abuse Handler tool are matched and mapped with the Category of illegal content.

Abuse Handling of Cloudflare

When a third-party abuse notifier sends an abuse notification to Cloudflare (instead of directly to Leaseweb), the abuse notifier will only be informed by Cloudflare that the reported domain (URL) belongs to a cloud infrastructure provider like Leaseweb. In doing so, third-party abuse notifiers are required to make use of the required Abuse Form made available by Cloudflare.

By using this Cloudflare Abuse Form, the cloud infrastructure provider (like Leaseweb), as a trusted partner to Cloudflare, will receive from Cloudflare the actual IP address that is involved with the reported domain (Cloudflare will not provide the IP address to the abuse notifier themself, since the IP address will be provided only to the cloud infrastructure provider responsible for the IP used upon its request.)

Since Cloudflare provides reverse proxy services, amongst others, the true IP address of a domain will be "masked" by the IP address of Cloudflare. The domain will point to a Cloudflare name server IP address. So, for an efficient and smooth processing of the reported abuse notifications by such third-party abuse notifier, Leaseweb requires that the third-party notifier use this Cloudflare Abuse form since

3. Leaseweb as a Good Hoster

Leaseweb's Abuse Handler needs a Leaseweb IP address to identify the responsible account operating or hosting the abusive specific domain.

Per Article 15.1 e) DSA information of the Leaseweb automated tools for the abuse handling procedures with indicators of the accuracy and the possible rate of error of the automated means used and any safeguards applied, is referred to in Chapter 3: Good Hoster reflecting minimized errors by means of automated tools combined with procedures for manual care whereby the related EU Templates Part. 8 (for tool based content moderation as automated means) (DE, NL) are exempt to the unmanaged IaaS operating model.

4. Notices – Illegal Content – Notice and Take Down Process

Leaseweb NL was one of the founding members of the NTD ("Notice and Take Down Procedure") in the Netherlands and is one of its proud endorsers of clean networks together with various other hosting and telecom parties in the Netherlands. Via its active memberships of the Dutch Cloud Community by Leaseweb NL, on its turn participating in the Anti-Abuse Network and joining with the Ministry of Justice to combat bad hosters, it is actively applying the NTD Abuse handling Code of Conduct. Also, Leaseweb is an ECO member for Leaseweb DE for more than 20 years, such membership provides for professional developments in the field of abuse handling, law enforcement, and keeping track of CSEM regulatory affairs. The Leaseweb Legal Department is converting new developments into legal requirements in the Policies adopted by Compliance.

Specifically, Leaseweb NL participated in the special addendum of the Dutch Notice and Take Down procedure concerning the swift and solid takedown of reported CSEM abuse notifications by OFFLIMITS. Leaseweb NL is also a sponsor of OFFLIMITS and applies the hash check filter deployed by OFFLIMITS to certain customers of Leaseweb NL. OFFLIMITS has been formalised as Trusted Flagger and appointend into 2025, where as OFFLIMITS was always considered a trusted flagger by Leaseweb internally.

The various and diverse participating Member States and Market Parties that apply the Notice and Take Down procedure ensure it meets both the requirements of the abuse notifiers (those who want to take content down), as well as the requirements for the notified parties (those who need to take the content down).

The sector involved in the Notice and Take Down and the proper execution of the Digital Services Act is continuously working on fair and reasonable orientation including taking part in the Internet and Jurisdiction Policy Network, Regulatory and Legal Track of the Internet Infrastructure Forum held in London (February 10-11, 2026) and earlier meetings for the same purpose, on diligence with the DSA legal requirements for online intermediaries and hosting providers.

The CRS (Customer Reported Solution) Rates for the Leaseweb DSA Transparency Report 2025 were achieved for abuse notifications received by Leaseweb NL and Leaseweb DE, respectively.

Leaseweb Entity	Customer Reported Resolution
Leaseweb NL	99%
Leaseweb DE	98%

The Compliance team makes a continued and rigorous undertaking in ensuring that customers live up to and be compliant with the Notice and Take Down timelines as required under the Leaseweb Policies to resolve the reported abuse notifications. Each abuse notification has a deadline for a Take Down. The Compliance department puts a lot of effort into a high Customer Reported Resolution Rate and a swift takedown of reported illegal content online, whereby Leaseweb services are used to strive for the shortest Uptime. Under the Leaseweb Compliance Policies, customers are also required to apply the Notice and Take Down Policies to their end-customers and users to resolve any abuse notifications within the same deadlines and aim for such Uptime.

Leaseweb Sales Entities, including Leaseweb NL and Leaseweb DE as Good Hosters, require having every abuse notification resolved within (at most) 24-48 hours, whereby this deadline is included in the abuse notification sent out. In some specific cases, a faster resolution time is fiercely demanded by Leaseweb based on its Policies.

The Customer Reported Solution Rate is based on the number of abuse notifications that are resolved in the Abuse Handler by the customer, for that reason referred to as Customer Reported Resolution. Therefore, the importance of this Customer Reported Resolution as high resolution rate means that as the notified abusive content has been resolved by the party responsible for such illegal content online, striving for a success rate of approximately 100% by

4. Notices – Illegal Content – NTD

each of the Leaseweb Sales Entities under the Leaseweb Policies and Notice and Take Down procedures. This Take Down responsibility is a mandatory step for every customer, resellers included, under the Leaseweb Policies.

Each year, Leaseweb strives to meet similar high Customer Reported Resolution Rates. This Customer Reported Resolution Rate is a result of strict deadlines applied by the Compliance team, and by providing constant instructions to Leaseweb customers to remove the notified abusive illegal content online. The customer is required in a transparent way, easy to understand, and explained with the 'know-how' to ensure that any abuse generated by illegal content (data) online, via their customer services in the Leaseweb network, is resolved and, where possible, prevented in the future.

The remaining approximately one percent (1%) of the Customer Reported Resolution Rate, while striving for 100%, consists of abuse notifications that are still in progress, being handled by the Compliance Department, manually actioned in shorts, pending.

Resolving these remaining abuse notifications of this one percent (1%) minimized magnitude is a result of duly and repeatedly notified deadlines based upon warnings including feasible disciplinary measures such as null routing (disrupting IP connectivity), suspending services, or as a last resort, full termination of the services agreement in the Leaseweb network as the sole remedies available for a (unmanaged) IaaS operating model in addition to the actions taken upon the Notices for Customer Reported Solutions.

As per Article 15.1 c) DSA information on engagement in content moderation is provided by clarifications that content moderation is not part of the operating model of IaaS service providers like Leaseweb DE and Leaseweb NL, by means of descriptions of the abuse handling process, the compliance team organization, the availability, visibility and accessibility of such information provided to the recipients of the service (meaning customers) and the Notice and Take Down, the partially automated NTD tool, categorized by the type of illegal content or violation of the terms and conditions (Policies), and by the type of restriction, is referred to in Chapters 2, Chapter 3 and Chapter 4 whereby the related EU Templates Part. 5 (own initiative content moderation based on illegal content) and EU Template Part. 6 (own initiative content moderation based on terms and conditions) (DE, NL) are both exempt to the unmanaged IaaS operating model. As outlined in the Chapters mentioned hereby, Leaseweb has clarified its Illegal Content Governance and has provided insight into its automated tools for its Customer Reported Solutions, matching with the IaaS operating model.

The relevant Notices are filled in and uploaded in EU Template Part. 4, filled in, see below.

Per Article 15.1 b) DSA listing the number of notices submitted in accordance with Article 16 DSA, categorized by the type of alleged illegal content concerned, including the number of notices submitted by Trusted Flaggers, all actions taken based on the law and the applicable terms and conditions, all processed by using automated means and the medium time needed for taking the action, is referred to in this Chapter 4 whereby the related EU Templates Part. 4 Notices (DE, NL) including Trusted Flaggers are filled in and uploaded including clarifications given on the Categories of Illegal Content online and Median time to take Action.

With respect to EU Templates Part. 4, please note that, considering the pre-listed Categories of Illegal Content, the following clarifications apply to the submitted Notices:

- DDoS, Hack, Gambling, Malware, Spam, VoIP, Zoophilia are listed under Other as no Illegal Category
- DDoS, Hack, Malware, Spam are Cyber abuse notices in Other, not listed as DSA illegal Content
- Median time to take Action (MttA): is the deadline given to achieve the Customer Reported Solution.
  - 24 hours
  - 1 hours
  - Median Time to Action (MttA): is the deadline given for CRS, and in the event needed, null-routing, suspension, and/or termination of services, which are deemed included.
    o Abuse Handler tool processing time of 60 seconds

4. Notices – Illegal Content – NTD

is excluded from MTTA, as per Annex 2.

- Categories of Illegal Content for the IaaS operating model and abuse handling (not meaning content moderation) are reflected in the filled in and uploaded selected categories of illegal content Notices.
- Categories of Illegal Content for Notices not being matched are not part of the EU Template Part. 4.

5. Law Enforcement and Member State Orders

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 and use their powers to engage with Orders to third parties like online intermediaries and hosting providers. This results in the need for Member State Authorities to perform investigations in the digital realm using their local Member State Authority powers, subject to specific jurisdictions, often using the IP address owner to issue Orders for secretive, highly regulated requests.

Leaseweb honors all Law enforcement requests. Leaseweb takes Law enforcement orders, including demands from Member State authorities, seriously, and each request is carefully reviewed by Leaseweb's Compliance Department, supported by the In-House Legal Department. In addition, local law firms are supporting Leaseweb in execution.

Therefore, the Compliance Department work closely with subject matter law firms and the in-house Legal department in each respective jurisdiction of Leaseweb NL and Leaseweb DE to examine the validity of the request and competency, as well as the legitimate powers of the law enforcement authorities. This is fully in line with the requirements under the DSA. In case relevant and appropriate, Leaseweb challenges the Order. On legitimate grounds, any incomplete, invalid, or unauthorized requests cannot be processed as rejected.

While being strict and diligent in validation of the Member State Order, Leaseweb also values, understands, and supports the important work done by law enforcement authorities and judicial authorities in their digital investigations.

Per Article 15. 1 a) DSA (jo Article 9-19 DSA) listing the number of orders to act and to provide information received from Member States authorities, the number of orders received from Member States authorities, is referred to in Chapter 5: Law Enforcement whereby the related EU Templates Part. 3 Member State Orders (DE, NL) are filled in and uploaded including clarifications given that no Categories of Illegal Content are provided in such Member State Orders. As listed, most law enforcement requests are for customer details.

Important to mention is that the Member State Order will list and include the statutory powers for the Member State authority to execute its investigations; however, the Member State Order does not contain any indication or reference to the Category of Illegal Content. Leaseweb is not informed of the Category of Illegal Content, whereby the only legal grounds provided are based on the statutory grounds of the Order.

6. Regulatory Matters

Leaseweb's anti-CSEM Policies

Leaseweb, as Good Hoster believes it is important to leave a positive footprint within the online community, and we take combating CSEM and exploitation very seriously. We strive to keep open communication and direct cooperation with respective hotlines for these specific topics, both inside and outside Europe. These hotlines carry the burden of the heavy task of evaluating CSEM content that individuals and organizations report to them. Leaseweb is always open to discussing how we can further improve our support based on our continued undertakings for CSEM reduction. Annually, Leaseweb has a constructive Sponsor meeting with OFFLIMITS to support its Good Hoster status.

Leaseweb requires the average Uptime is around 1.5 hours, meaning that abuse notifications for CSEM content are taken down from the internet (NTD) within the Leaseweb CSEM deadline of a maximum of 1 hour, referred to as Median time to take Action in EU Template Part.4 Notices and Trusted Flaggers.

As a result, over the past years, in applying this strict policy, certain domains moved away from the Leaseweb network on their own initiative. In practice, and unfortunately, illegal material seems to be inevitable.

OFFLimites Instant Image Identifier (3Is)

To jointly stand up against CSEM, Leaseweb works together with the expert desk in the Netherlands, OFFLIMITS, in 2026, formally established as Trusted Flagger, and encourages the active installation of the HashCheckService, renamed as Instant Image Identifier ("3Is"), as a requirement for third-party user-generated content infrastructures that utilize Leaseweb's network. Leaseweb – as sponsor of OFFLIMITS – fully supports the further development and engagement of OFFLIMITS with the hosting industry.

The Leaseweb Policies include the mandatory use of the 3Isas as part of the Leaseweb Compliance program for its customers, including resellers, such as Cloud Storage Providers and other user-generated content websites. Additionally, Leaseweb requires its customers to implement and pursue this obligation to use the 3Is back-to-back by their clients (end users of their user-generated services) as a mandatory condition of the Leaseweb Policies and the legitimate use of the Leaseweb services; this is all included in the Policies.

In the draft EU Regulations laying down the Rules to prevent and combat CSEM, still in European regulatory debate and under fierce political impact, Leaseweb, as a member of CISPE, strives to clarify its role of online intermediary, as demonstrated in the CISPE Position paper on the CSEM regulatory proposals https://www.cispe.cloud/csam and the very clear video to demonstrate the regulatory focus for CSEM.

Click here for more info

Visit CISPE website for more info

END OF DOCUMENT

Get in Touch

www.leaseweb.com info@leaseweb.com in/company/leaseweb f/leaseweb