

COMPLIANCE TRANSPARENCY REPORT

VERSION ISSUED BY THE LEASEWEB GLOBAL
LEGAL & COMPLIANCE DEPARTMENT
NO. 1

TABLE OF CONTENTS

| | |
|---|-----------|
| 1. Introduction and Goals | 3 |
| 2. Leaseweb as a Good Host | 4 |
| 3. Abuse Handling | 5 |
| 3.1 Leaseweb Compliance Department | 5 |
| 3.2 Notice and Take Down Process | 5 |
| 3.3 Automated Abuse Handling System | 5 |
| 3.5 Compliance Rate | 6 |
| 4. KYC Department | 7 |
| 5. Law Enforcement | 8 |
| 6. Regulatory Matters | 9 |
| 7. Focus on Removing CSEM in the Netherlands | 11 |
| 7.1 Leaseweb's Anti-CSEM Policies | 11 |
| 7.2 EOKM HashCheckService Filter | 11 |
| 7.3 Dutch Ministry of Justice and Security Combatting CSEM | 13 |
| 7.4 The Focus of the Ministry of Justice and Security in 2020 | 13 |

To report an abuse notification with Leaseweb Sales Companies, please visit: www.leaseweb.com/abuse-prevention

For media/press contact, please visit:
[Leaseweb](#) or send an [email](#)

1. Introduction and Goals

This Compliance Transparency Report aims to provide Leaseweb customers and relevant and interested parties, such as government, law enforcement authorities, and business partners, a realistic and genuine activity-based overview of Leaseweb's Compliance approach to Internet Abuse Handling, or a so called misuse of Internet.

Leaseweb is a leading Infrastructure as a Service (IaaS) provider serving a worldwide portfolio of 18,000 customers ranging from SMBs to Enterprises. Leaseweb's 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.

The company operates 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.

Leaseweb offers services through its various independent sales companies including: Leaseweb Netherlands B.V. ("Leaseweb Netherlands"), Leaseweb USA, Inc. ("Leaseweb USA"), Leaseweb Asia Pacific PTE. LTD ("Leaseweb Asia"), Leaseweb CDN B.V. ("Leaseweb CDN"), Leaseweb Deutschland GmbH ("Leaseweb Germany"), Leaseweb Australia Ltd. ("Leaseweb Australia"), Leaseweb UK Ltd ("Leaseweb UK"), as well as Leaseweb Hong Kong Ltd ("Leaseweb HK") and Leaseweb Japan K.K. to be added soon "Leaseweb Japan" (all together "Leaseweb Sales Companies").

For more information visit: www.leaseweb.com.

The above listed Leaseweb Sales Companies operate under local applicable law, whereas the EU-based high level standards, including GDPR, are the leading policy of the EU-based Leaseweb headquarters.

It's important to note, that Leaseweb Netherlands was one of the first hosting providers to release a Transparency Report in 2013 for the Netherlands, merely focused on law enforcement requests and statistics.

This re-introduction of the Transparency Report by Leaseweb has a more comprehensive format since it covers the spectrums of Abuse Handling and compliance for all its Leaseweb Sales Companies and it's not focused on the quantitative information about law enforcement requests from authorities only.

This Transparency Report presents how Leaseweb cares for Compliance and undertakes Internet Abuse Handling with a high Compliance Rate.

With this Transparency Report, Leaseweb intends to release an overview with a focus on Internet compliance open for the public with a more general approach on the topic of Internet misuse, and especially informative for the Leaseweb customer, authorities, foundations that support in Abuse Handling and anyone else interested in Leaseweb as a good hoster.

In this Transparency Report, Leaseweb explains the setup of the Compliance department responsible for handling all incoming abuse notifications for Leaseweb Sales Companies, including difficult categories of Internet misuse that are cause for public debates.

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.

The success of the Compliance department is measured by the Compliance Rate, meaning the speed of resolving abuse notifications by each of the Leaseweb Sales Companies.

2. Leaseweb as a Good Hoster

Leaseweb is a diversified Internet service provider, 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 content services. Leaseweb, for example, does not manage 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.

Due to its size, quality, and pricing, all Leaseweb Sales Companies are an attractive hosting provider for bandwidth-intensive, user-generated content sites, where users can share and contribute content.

Leaseweb sets out the policies for its customers 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 [here](#).

As an IaaS hosting provider, we do not have access to the content of customers' services and depend on external feeds and abuse notifications from third parties to become aware of any Internet misuse taking place in the Leaseweb network.

At Leaseweb we take a proactive approach where possible to our network health. We seek and reach out to foundations and organizations (so called 'Feeds'), who 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 Companies receive input from a variety of Feeds such as: Spamhaus, ShadowServer, EOKM, Phishtank, Abuse.ch, Spamcop, Netcraft, Phishlabs, RSA, Botnet Tracker, Bitninja and many more. Whenever a Feed is available, the Compliance team will investigate possibilities to subscribe to it, or to receive the input in an alternative way. All of these Feeds are imported into the Abuse Handler and are processed automatically.

By subscribing to such Feeds there is an expected increase in the number of abuse notifications. The combination of abuse Feeds and abuse notifications mentioned above, allows us to identify patterns of abusive behavior that we can act upon. For example bringing to light the so called 'repeating offenders' that allows Leaseweb Sales Companies to take appropriate actions.

Within our network such Feeds also provide a better understanding and more insight into the health of the Leaseweb network, which is necessary for our good hoster position, with over 18,000 customers worldwide and continuously growing.

It matters how compliant a hoster is with the received abuse notifications. For a good hoster, from the Compliance point, the 'Uptime' (how long the reported content stays online and how fast it will be resolved) is a main KPI and measure of success.

We consider the total number of abuse notifications, or reported websites or domains, subjective, as it's fully dependent on the size of the network and the number of customers.

It's important to note that the number of abuse notifications itself does not determine whether a provider is a good hoster or a bad hoster. The larger the business, the more abuse notifications.

As stated in the Introduction, the success of the Compliance department is measured by the Compliance Rate, meaning the speed of resolving abuse notifications by each of the Leaseweb Sales Companies, and the Uptime combined.

All Leaseweb Sales Companies adhere to strict internal Compliance Policies that are aligned with the requirements of local laws and are applied globally. As a good hoster, Leaseweb applies these strict Compliance Policies to achieve our high Compliance Rate and short Uptime.

More details are provided later in this Transparency Report.

3. Abuse Handling



3.1 Leaseweb Compliance Department

Leaseweb has a dedicated Compliance team to maintain a healthy network, dealing with copyright holders, copyright agencies, law firms, law enforcement authorities, foundations and organizations focused on Abuse Handling and anyone else who files an abuse notification. The Leaseweb Compliance department regularly attends conferences and know-how related taskforces in the Abuse Handling and Know Your Customer fields.

3.2 Notice and Take Down Process

Leaseweb Netherlands was one of the founding members of the NTD ('Notice and Take Down Procedure') and is one of its proud endorsers, together with various other hosting and telecom parties in the Netherlands.

Specifically, Leaseweb Netherlands participated in the new addendum of the Dutch Notice and Take Down procedure concerning the swift and solid takedown of reported CSEM abuse notifications by EOKM ('Expertisebureau Online Kindermisbruik', or 'Meldpunt KinderPorno' / 'KP').

The various and diverse participating 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 current Notice and Take Down Procedures, for example, can be found [here](#).

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. It includes the obligations Leaseweb is requiring from third parties to properly execute the Notice and Take Down Procedures under the Leaseweb Policies and applicable law, such as the EU e-Commerce Directive section 14. For more information about the Regulatory applicable law, please see Chapter 6: Regulatory.

3.3 Automated Abuse Handling System

The performance of the Notice and Take Down Procedures starts with the third-party abuse notification: The Notice. The processing of these abuse notifications is in line with regulations and Leaseweb Policies under the Notice and Take Down Procedures.

In case an abuse notifier has a reason to send an abuse notification, any abuse email address of any of the Leaseweb Sales Companies is available on the Leaseweb website.

Leaseweb carefully explains to abuse notifiers that a valid Leaseweb Internet Protocol (IP) address needs to be included in the abuse notification. This is required to successfully match the abuse notification with the account that is using the Leaseweb network. Without a valid Leaseweb IP address the abuse notification cannot be matched, which delays any further processing of the abuse notification.

Every abuse notification sent to any of the abuse email addresses of the Leaseweb Sales Companies is automatically processed and evaluated by our state of the art, in-house developed Abuse Handling system. The Compliance team works with this Abuse Handling system as a tool, deploying seasoned experience and know-how. The Abuse Handler processes notifications 24/7, 365 days a year for all of the Leaseweb Sales Companies. Every received abuse notification is forwarded, after automated evaluation of the content and keywords, without any interference resulting in a continuous and swift processing of abuse notifications. The Compliance team handles all follow up communication and manually addresses any abuse notifications that require specialized attention to ensure safety is taken into consideration.

3.4 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 hosting provider like Leaseweb. In doing so, the third-party abuse notifiers are required to use the Abuse Form made available by Cloudflare.

3. Abuse Handling



By using the Cloudflare Abuse Form, the hosting provider (like Leaseweb) and 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 themselves, since the IP address will be provided only to the hosting provider upon its request.

Since Cloudflare is used to providing a secure environment for a website, it protects against spam and DDoS attacks. The true IP address of a domain will be 'masked' by an IP address of Cloudflare. The domain will point to a Cloudflare IP address.

For an efficient and smooth processing of the reported abuse notifications by such third-party abuse notifier, Leaseweb requires that the third-party notifier uses the Cloudflare Abuse form. That's because the Leaseweb's Abuse Handler needs a Leaseweb IP address to identify the responsible account operating or hosting the abusive domain.

3.5 Compliance Rate

Leaseweb appreciates and values a high Compliance Rate, meaning, the resolution of the abuse notifications within the deadlines required by Leaseweb or the so called Uptime: the Take Down. The Leaseweb Compliance Rate is based on the number of notices that is reported as Taken Down and resolved in the Abuse Handler system within the applicable required deadlines, or the Uptime.

As part of Leaseweb's services, the Compliance team makes a continued and rigorous commitment to ensuring customers resolve the reported abuse notifications, and live up and stay compliant within the Notice and Take Down timelines, as required under the Leaseweb Policies. Each abuse notification has a deadline for a Take Down. The Compliance department puts a lot of effort into a high Compliance Rate and a swift takedown of reported content to ensure a short Uptime.

Under Leaseweb Policies customers are also required to demonstrate that they apply Notice and Take Down policies to their end customers to resolve any abuse notifications within the same deadlines and ensure the short Uptime.

Leaseweb Sales Companies - as a responsible, good hosting provider - require having every abuse notification resolved within (at most) 24-48 hours, where this deadline is included in the abuse notification. In some specific cases, a faster resolution time is fiercely demanded by Leaseweb based on its Policies. For example, Leaseweb applies a strict timeline of only one (1) hour for CSEM abuse notifications, as a maximum Uptime.

The Compliance Rate is based on the number of abuse notifications that are resolved in the Abuse Handler and taken down.

A successful Compliance Rate means that the notified abusive content has been resolved and taken down within the deadlines by the party responsible for such content. Each of the Leaseweb Sales Companies under the Leaseweb Policies and Notice and Take Down procedures strives for the success rate of approximately 100%. This Take Down responsibility is a mandatory step for every customer, including resellers, under Leaseweb Policies. In 2019, a Compliance Rate of 99,0 % was achieved for all abuse notifications received by the Leaseweb Sales Companies.

Each year, Leaseweb strives to meet a similar high Compliance Rate. The Compliance Rate is a result of strict deadlines set by the Compliance team, and by providing constant instructions and support to Leaseweb customers in removing the notified abusive content. The customer is guided with the 'know-how' to ensure that any abuse generated content (data) on their services in the Leaseweb network is resolved and, where possible, prevented in the future.

The remaining percentage of approximately one (1%) of the Compliance Rate - while striving for 100% - consists of abuse notifications that are underway and in progress driven by the Compliance department, and are actually handled for Take Down, since given deadlines have expired. Resolving these open abuse notifications may involve heavy disciplinary measurements, such as null routing, shutting down of services, or, as a last resort, full termination of the contractual agreement for the service in the Leaseweb network.

4. KYC Department

At Leaseweb, the Compliance department is not only an abuse desk. The KYC process is an integral part of the Compliance department's responsibilities and it benefits the onboarding of new customers.

The Compliance department is the gatekeeper of approving new customers, managing the customer verification process, focused on neutral, objective KYC control. The purpose of the KYC process is to identify any potentially abusive behavior prior to undergoing contractual agreements, and ensuring a healthier network and good hosting performance, that constitute reliable hosting.

Benefits of having the KYC process within the Compliance department:

- The trained Compliance team works in automated systems and can quickly identify abusive and fraudulent ordering behavior
- Fraudulent ordering and malicious use of services can be successfully avoided
- Upon termination of a repeating abuse offender, the team provides the instant possibility to improve the customer verification process to avoid similar new accounts
- The team provides insights into the ID, valid details and type of businesses of the customer, including resellers

This customer verification is embedded in a smooth onboarding process for new customers, enhancing the customer experience and the swift delivery of Leaseweb services.

5. Law Enforcement

The growth of online activity has caused a rise of cybercrime, posing 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 specific jurisdictions. The reason that law enforcement authorities reach out to hosting companies, like Leaseweb, is to track and trace 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.

Leaseweb Sales Companies take any Law enforcement orders and demands seriously and each request is carefully reviewed by Leaseweb's Compliance team. The team of legal and compliance specialists work closely with external law firms and counsels in each jurisdiction of the Leaseweb Sales companies to examine each request for validity and competency as well as legitimate powers of the law enforcement authorities. 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 statistics and absolute numbers to the extent permitted by local law (like in some other transparency reports of content platforms) Leaseweb provides transparency of our position as an IaaS unmanaged cloud hosting provider (not a content platform) towards law enforcement authorities.

Leaseweb values, understands, and supports the important work done by law enforcement authorities and judicial authority in their digital investigations, and strives to build up a sound and appropriate cooperative relationship. At the same time Leaseweb will always apply its high values on due diligence, and provide assistance in case of valid orders required by law.

The amount of law enforcement orders and demands vary per jurisdiction of the Leaseweb Sales Company based on their legal system. For example, in a certain jurisdiction the legal system generates a high amount of orders for law enforcement that are produced and submitted to hosters like Leaseweb, compared to another jurisdiction where the legal grounds for such orders may vary.

6. Regulatory Matters

Most Internet regulated jurisdictions provide safe harbors for hosting providers, to shield them from liability for content that is hosted on the hoster's network. Within the European Union ('EU'), these principles are laid down in the E-commerce Directive, and in the United States in the Digital Millennium Copyright Act ('DMCA'). As a condition to be entitled to the protection of the safe harbors, the hosting provider must have a passive role in regard to the content, and duly and carefully act upon abuse notifications that it receives. Safe harbor provisions shield hosting providers and website operators from general liability.

Leaseweb as a neutral IaaS ('Infrastructure as a Service') provider, whose services consist of transmission, caching and storage of information provided by customers, with its safe harbor hosting immunity as online intermediary, is not under any general obligation to monitor or to research for circumstances that would indicate unlawful activity, or to take measures to actively investigate or monitor for potential illegal activity, or to stop potential illegal activity prior to any notice.

As the conditions in article 14 of the E-Commerce Directive make apparent, the hosting safe harbor immunity based on the mere conduit service provided by Leaseweb, relies heavily on the Notice and Takedown Procedure ('NTD'). Under this NTD procedure, whenever a hosting provider receives a complaint – a Notice – the hosting provider only benefits from a liability exemption, provided they 'act expeditiously' to remove or disable access to the illegal or unlawful content on their servers. In the SABAM landmark judgement, the European Union Court of Justice ruled that Internet service providers cannot be ordered to install a general filtering system to prevent any infringement of intellectual property rights.

As clarified, a hosting provider can benefit from the safe harbor detailed above, if it has a passive role regarding the content. However, if the hosting provider starts scanning content, it's no longer passive and may lose the protection offered by the safe harbor. In other words, scanning content has major legal implications. This way, any good intention to monitor content may result in increased liability for the

hosting provider regarding the content in its network. In addition, under EU privacy legislation, deep packet inspection is only allowed under strict conditions. One of the conditions is that all data is anonymized. However, any anonymization would render the scanning unusable for the aim of banning illegal content. The current complex regulatory landscape with its evolving compliance regulations requires Leaseweb to stay current on the latest news and regulations.

Leaseweb is required to anticipate any regulatory trends in the future, such as the upcoming Digital Services Act ('DSA') – that will update the two decades old E-Commerce Directive and adopt new rules governing the EU based Internet and Terrorist Content Online Regulation ('TCO').

Leaseweb cares to demonstrate to regulatory authorities that its role as an IaaS hosting provider and online intermediary should be defined in a specific manner, with deviation and exemption from any other cloud hosting provider definition.

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-removal of content including legitimate content is an inevitable consequence or risk that should be solved by any measures proportionate to the threat, meaning Notice and Take Down actions must specifically target the illegal content in question and avoid indiscriminate removal of legitimate and legal customer content. This approach should be included in the DSA and TCO.

¹ Articles 12-15 of the Directive 2000/31/EC, also known as the 'E-commerce Directive'.

² Scarlet Extended SA v. SABAM (C-70/10).

6. Regulatory Matters

In the draft TCO regulation all of the above is proposed in the following definition that applies to Leaseweb as an online intermediary service with an emphasis on infrastructure: 'Cloud infrastructure services' which consist in the provision of on-demand physical or virtual resources, that provide computing and storage infrastructure capabilities, independently managed by end users, as to what content is stored or made publicly available. The IaaS service provider does not have the necessary technical access to remove specific content stored by end users or by the end users of such customers without disabling, suspending or terminating the service used by other customers or their end users, proposing that the position of the IaaS online intermediary shall not be considered within the meaning and for the purposes of this TCO Regulation.

Leaseweb's memberships and alliances with hosting organizations (DHPA, DINL and the EU based CISPE), help 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, to ensure ongoing compliance with current and future regulations.

Leaseweb prepares for any impact arising from new regulations and the effect it might have on our operations, for a seamless implementation of these new regulatory frameworks.

7. Focus on Removing CSEM in the Netherlands

7.1 Leaseweb's Anti-CSEM Policies

Leaseweb as a good hoster believes it's important to leave a positive footprint within the online community, and we take combatting online child abuse and exploitation very seriously. We strive to keep open communication and direct cooperation with respective hotlines for these specific topics, both inside and outside of 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 discuss how we can further improve our support, based on our continued undertakings for CSEM reduction.

Unquestionably, CSEM is prohibited, illegal and strictly banned under Leaseweb Policies. Many years ago, Leaseweb Netherlands took the decision to also ban non-illegal child erotica content from the Leaseweb network, meaning any legal, however suggestive material, which depicts children in a sexualized manner or context. Even though child erotica does not meet the threshold for legal prohibition in many countries. We believe this is a helpful, preventive deterrent, which serves as a discouragement for third parties that want to host and distribute such content.

In addition to making this internal decision of not tolerating such equally disturbing child erotica content, Leaseweb introduced a very strict deadline for all our Sales Companies to take down the reported abusive content. We demand to take the reported abusive content concerning children offline within 1 hour. Failure to do so leads to Leaseweb's service interruption, to immediately disable the CSEM content.

Regarding CSEM specifically, Leaseweb identified that this type of abuse is mainly observed in Cloud Storage Providers ('CSP') infrastructures, generated by third-party end users uploading the abusive content. Most CSEM abuse notifications are related to CSP, who in return depend on user-generated content, meaning that third-party users can upload any type of content, often free of charge.

CSPs are lawful and legitimate, they are used for storage and uploading of any material, including legal material, such as holiday photos to share with friends and family, and unfortunately also illegal material such as CSEM, like any type of service that allows for user-generated content.

Leaseweb contributes to fighting this problem in society by requiring and demonstrating that the average Uptime is around 1.5 hours, meaning that abuse notifications for CSEM content are taken down from the Internet within the Leaseweb CSEM deadline of maximum 1 hour.

As a result of this strict policy application, certain domains moved away from the Leaseweb network on their own initiative over the past years. Unfortunately in practicality, illegal material seems to be inevitable.

7.2 EOKM HashCheckService Filter

As one of the first Dutch IaaS providers, Leaseweb Netherlands discussed with EOKM to receive the non-illegal child erotica abuse notifications to combat such content under the Leaseweb Policies, along with receiving abuse notifications for CSEM ('Child Sexual Exploitation Material') that covers obvious and explicit forms of child sexual abuse and exploitation as illegal content.

EOKM has introduced the HashCheckService which is a service with a database that contains hashes of known CSEM material based on the MD5 Hash technique and Microsoft PhotoDNA, made available via an API. The database is made available by the Dutch police and contains content that is no longer being investigated and is considered 'known' CSEM material. The EOKM HashCheckService aims at preventing uploads of known CSEM images onto hosting services and platforms.

For example, user-generated image platforms, such as (exploited by) Cloud Storage Providers can implement this HashCheckService, meaning each uploaded file will be checked against the abusive collected files in the hash database. If there is a hit, the upload can be blocked.

7. Focus on Removing CSEM in the Netherlands

To jointly stand up against CSEM, Leaseweb works together with the expert desk in the Netherlands (EOKM) as a good hoster and encourages to actively install the HashCheckService as a requirement for third-party user-generated content infrastructures that utilize Leaseweb's network. Leaseweb – as a sponsor of EOKM – fully supports the further development and engagement of EOKM with the hosting industry.

Leaseweb Policies include the mandatory use of this HashCheckService as an obligatory part of the Leaseweb Compliance program for its customers and 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 HashCheckService by their clientele (end users of their user-generated services) as a mandatory condition of Leaseweb Policies and the legitimate use of Leaseweb services.

Leaseweb's Compliance department enforces the swift removal of this abuse content and works cooperatively with customers to jointly combat the proliferation of CSEM stemming from its beliefs as a good hoster.

Unfortunately, due to the nature of the Internet industry and strong networks, abuse by third-party user-generated content cannot be avoided in its totality, while providing services to other businesses and infrastructures from Leaseweb's unmanaged hosting business model.

Leaseweb has been a well-respected partner and sponsor of EOKM for many years and will strive together with EOKM to further optimize its Abuse Handling results against CSEM.

To illustrate the cooperation between EOKM and Leaseweb, where Leaseweb is presented as a good hoster, EOKM provided the following comment:

'For many years, there has been a good relationship between the EOKM and Leaseweb and their Compliance team. Their Compliance lead guides a large team of specialists focused on Internet misuse, including the handling of CSEM. Leaseweb was one of the founders of the Notice and Take Down initiative in The Netherlands and has continuously had a professional, effective, and very proactive approach to CSEM Abuse Handling.

Leaseweb's high compliance standards to prevent CSEM and going the extra mile to take down child erotica, makes Leaseweb one of the best hosters to work with in the fight against CSEM. Leaseweb applies a short takedown deadline of 1 hour to remove such content and applies a null route in cases of non-compliance. This practice is above and beyond the general standards and is much stricter than the requirement of removal within 24 hours.

As a result of this strict compliance policy, the Notice and Take Down procedure is mandatory and in practice well adopted by their customers. It is an obligation for their customers that are engaged with user-generated content to be connected to the EOKM HashCheckService. All of these standards make Leaseweb one of the leading parties in this field.

Moreover, Leaseweb, as our sponsor and reliable hoster, is a pleasure to work and communicate with and we welcome many years of fruitful cooperation together.'

- Mrs. A. Gerken, EOKM Director



7. Focus on Removing CSEM in the Netherlands

7.3 Dutch Ministry of Justice and Security Combatting CSEM

In 2018 an initiative was set by Dutch law enforcement and the Ministry of Justice and Security to reduce and prevent online child abuse. For years, the Netherlands has been mentioned as one of the top three countries, where most of the CSEM content is hosted. The Netherlands has become a target due to its strong Internet infrastructure which includes the location of AMS-IX, one of the most important Internet traffic hubs in the world, as well as an easy setup for Internet companies to operate. This results in an increased interest in the Netherlands for cybercriminal activities such as CSEM.

For surrounding countries, but also in our society, the clarification mentioned above is not a sufficient and acceptable answer to 'Why?' most CSEM content is hosted in the Netherlands. This has led to a great deal of debates on how the Netherlands should resolve this issue. This task was assigned to the Minister of the Justice and Security department and has resulted in several roundtable discussions with law enforcement, ministries and private parties from the hosting and telecom sector, including Leaseweb Netherlands.

As one of Europe's biggest hosting providers, Leaseweb Netherlands contributed to these roundtable sessions and provided input. These sessions concluded several initiatives, such as:

- Adding an Addendum on December 13th, 2018 to the existing NTD ('Notice and Take Down') procedure as executed by good hosters, where endorsed parties commit to a deadline of 24 hours to take down the CSEM material (note: Leaseweb Compliance Policies requires 1 hour take down);
- An administrative fine, if a hosting provider continuously does not remove the abuse content, notified by EOKM within the given deadline stipulated in the NTD Addendum, with the consequence of a fine for such bad hoster;
- The development of the HashCheckService filter operated by EOKM, which can be used by hosters that offer managed hosting and in case of unmanaged IaaS hosting provider like Leaseweb, they can apply it with services used by user-generated content platforms and websites.

7.4 The Focus of the Ministry of Justice and Security in 2020

The Ministry of Justice and Security continues with its focus on the handling of CSEM in follow up to the execution of the special Addendum in the NTD, that was signed by Leaseweb in 2018. The Ministry of Justice and Security led by Minister Grapperhaus keeps a great focus in the Netherlands to combat CSEM and lead by example in the European Union with the proactive approach. Leaseweb fully embraces and supports this approach, as it has been fully in line with Leaseweb's Compliance Policies for many years.

Leaseweb will continue to participate in private/public broad roundtables for these topics with the Ministry and will undertake all efforts to inform the Ministry of Justice and Security of its experience as a good hoster and its best practices.

Leaseweb contributes to this debate with the Ministry of Justice and Security and the TU Delft Monitor in cooperation with EOKM, and firmly advises the Ministry on the need to measure Uptime and make a solid definition of a good hoster, as opposed to a bad hoster.

The Ministry will then be enabled to instruct on the main principles of measuring Uptime to the TU Delft Monitoring team for the purpose of producing accurate and reliable statistics to identify good hosters and bad hosters.

Leaseweb's Compliance team and Management team will continue to embrace these anti-CSEM activities.



© October 2020

Compliance department - Leaseweb is the brand name under which the various independent Leaseweb companies operate. Each company is a separate and distinct entity that provides services in a particular geographic area. Leaseweb Global B.V. does not provide third-party services.

Please find more information [here](#)

Get in Touch

✉ info@leaseweb.com

[in /company/leaseweb](https://www.linkedin.com/company/leaseweb)

[f /leaseweb](https://www.facebook.com/leaseweb)