COMPLIANCE TRANSPARENCY REPORT LEASEWEB 2021

ISSUED BY LEASEWEB GLOBAL LEGAL & COMPLIANCE

VERSION: 1.0 – FEBRUARY 2022

TABLE OF CONTENTS

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. Introduction and Goals

This Compliance Transparency Report 2021 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, or 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. 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 Entities which are: 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"), Leaseweb Hong Kong Ltd. ("Leaseweb HK") and Leaseweb Japan K.K. ("Leaseweb Japan") (all together "Leaseweb Sales Entities"). For more information visit: www.leaseweb.com.

Above listed Leaseweb Sales Entities operate under local applicable law, whereby the EU based high level standards including GDPR, are leading policy by Leaseweb from its EU based head-office.

It is 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 of Leaseweb has a more comprehensive format since it covers the spectrums of abuse handling and compliance for all its Leaseweb Sales Entities and is not focused (only) on the quantitative information on law enforcement requests from authorities.

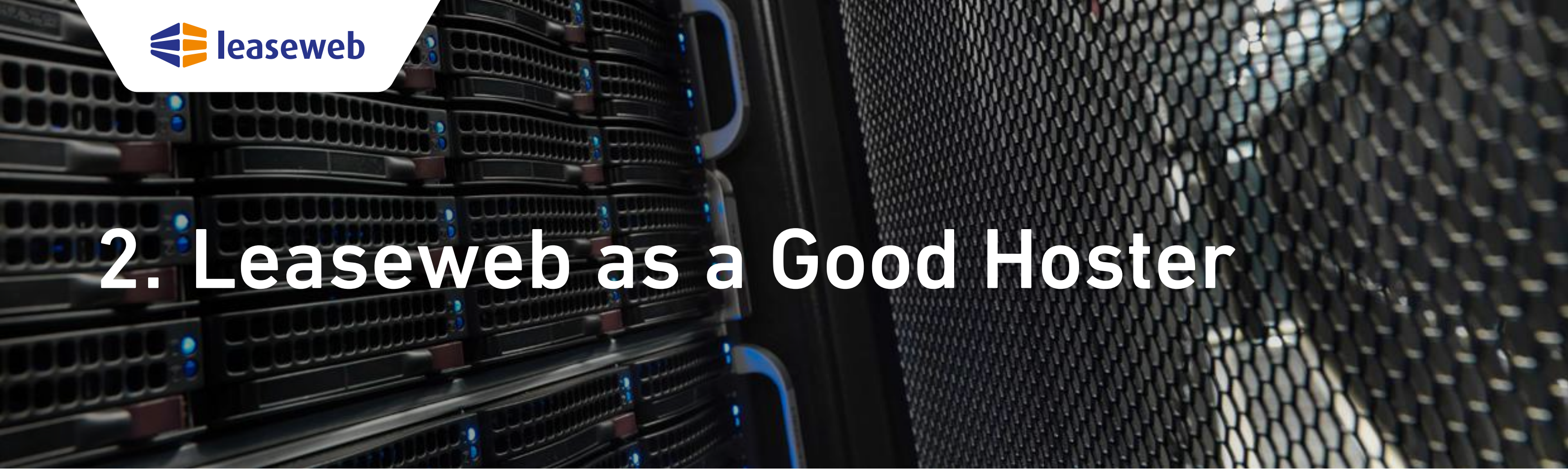
This Transparency Report presents how Leaseweb cares for Compliance and undertakes internet abuse with a high compliance rate.

Leaseweb intends to release with this Transparency Report an overview with a focus on internet compliance thereby open for the public with more general approach on the topic of internet misuse, and specifically 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 the Leaseweb Sales Entities, including difficult categories of internet misuse that are cause 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 mis-use.

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 Entities.



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 Entities are an attractive hosting provider for bandwidth-intensive, user-generated content sites, where users can share and contribute content.
Leaseweb -in its relationship with its customers- 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.
The policies will be updated from time to time, taking into account new regulations and 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.
As an IaaS hosting provider, we do not have access to the content on customers' 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.

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 their 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, ShadowServer, EOKM, Phishtank, Abuse.ch, 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 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 above-mentioned combination of abuse Feeds and abuse notifications, allows us to identify patterns of abusive behavior that we can act upon, for example bringing to light so called "repeating offenders" which allows the Leaseweb Sales Entities to take appropriate actions.

Within the network such Feeds also provide a better understanding and more insight in the health of the Leaseweb network, which we need for our Good Hoster position with over 20.000 customers worldwide and growing continuously. It matters how compliant a hoster deals with its received abuse notifications. For a Good Hoster, the "Uptime" (how long the reported content stays online and how fast it will be resolved) is a leading success KPI for Compliance.

We consider an absolute number of abuse notifications or reported websites or domains subjective, as it is fully dependent on the size of the network and the number of customers.

It is important to note that the number of abuse notifications itself does not qualify a Good Hoster or bad hoster: the larger the business, the more such abuse notifications.
Like 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 Entities and the Uptime together.
All Leaseweb Sales Entities 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.

More details are set out further 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 that files an abuse notification. The Leaseweb Compliant department annually attends conferences and know-how related taskforces in the knowledge field of Abuse Handling and Know Your Customer.

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 ensures 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 in: 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 and 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 with respect to 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 reason to send an abuse notification, any abuse email address of any of the Leaseweb Sales Entities 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 that is 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.

Every abuse notification sent to any of the abuse email addresses of the Leaseweb Sales Entities 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. This system, the Abuse Handler, processes notifications 24/7, 365 days a year for all the Leaseweb Sales Entities. 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. No doubt, and for safety's sake, the Compliance team handles all follow up communication and handles manually any abuse notifications that require specialized attention.

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, third party abuse notifiers are required make used of the required Abuse Form made available by Cloudflare. By using this Cloudflare Abuse Form, the hosting provider (like

3. Abuse Handling

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 hosting provider upon its request.)

Since Cloudflare is used to provide a secure environment for a website, it protects against such as spam/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.

So, for an efficient and smooth processing of the reported abuse notifications by such third-party abuse notifier, Leaseweb require that the third-party notifier uses this Cloud Flare Abuse form since the Leaseweb’s Abuse Handler needs a Leaseweb IP address to identify the responsible account operating or hosting a the abusive specific 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, the Uptime.

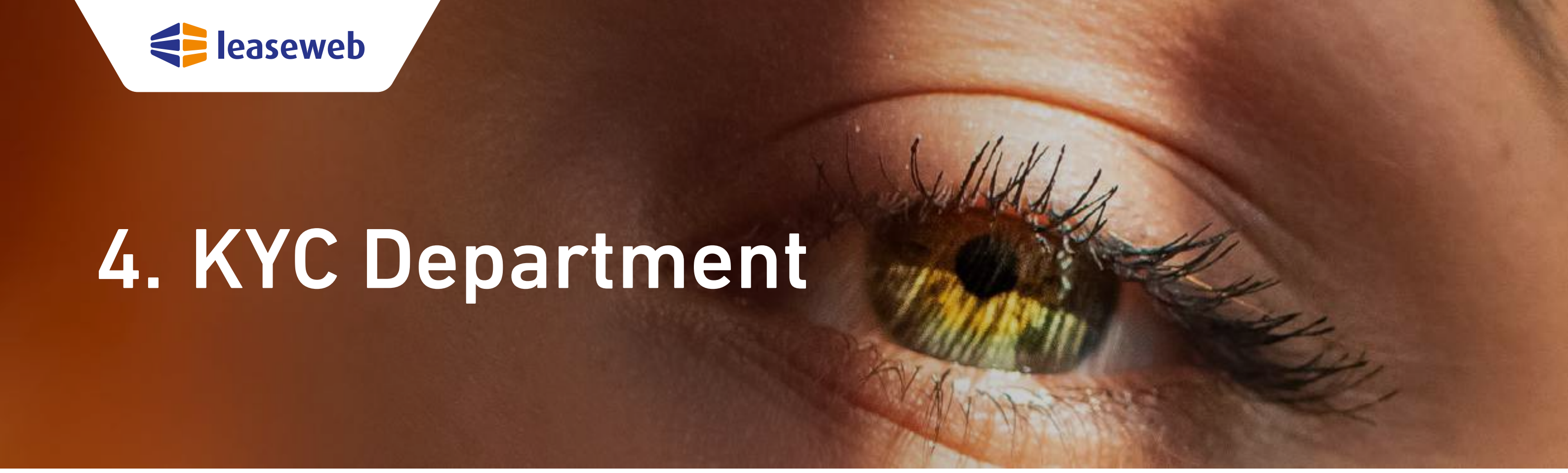
As part of Leaseweb’s services, the Compliance team makes a continued and rigorous undertaking in ensuring customers to live up and be compliant within the Notice and Take Down timelines as required under the Leaseweb Policies to resolve the reported abuse notifications. Each abuse notification has a deadline for a Take Down. The Compliance department puts a lot of effort into a high Compliance Rate and a swift takedown of reported content to ensure a short Uptime. Under the Leaseweb Policies, customers are also required to demonstrate and that they apply -on their turn- such 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 Entities - as a responsible good hosting provider - require having every abuse notification resolved within (at most) 24-48 hours whereby 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 the 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.

Therefore, the importance of this high Compliance Rate is the meaning that the notified abusive content has been resolved and Taken Down within the deadlines by the party responsible for such content, striving for the success rate of approximately 100% by 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. In 2019, the Compliance Rate of 99,0 % has been achieved, for all abuse notifications received by the Leaseweb Sales Entities.

Each year, Leaseweb strives to meet such similar high Compliance rate. This Compliance Rate is a result of strict deadlines 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 in progress by the Compliance department and actually being 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 merely an abuse desk. The KYC process is an integral part of the Compliance department's responsibilities and benefits the onboarding of new customers.

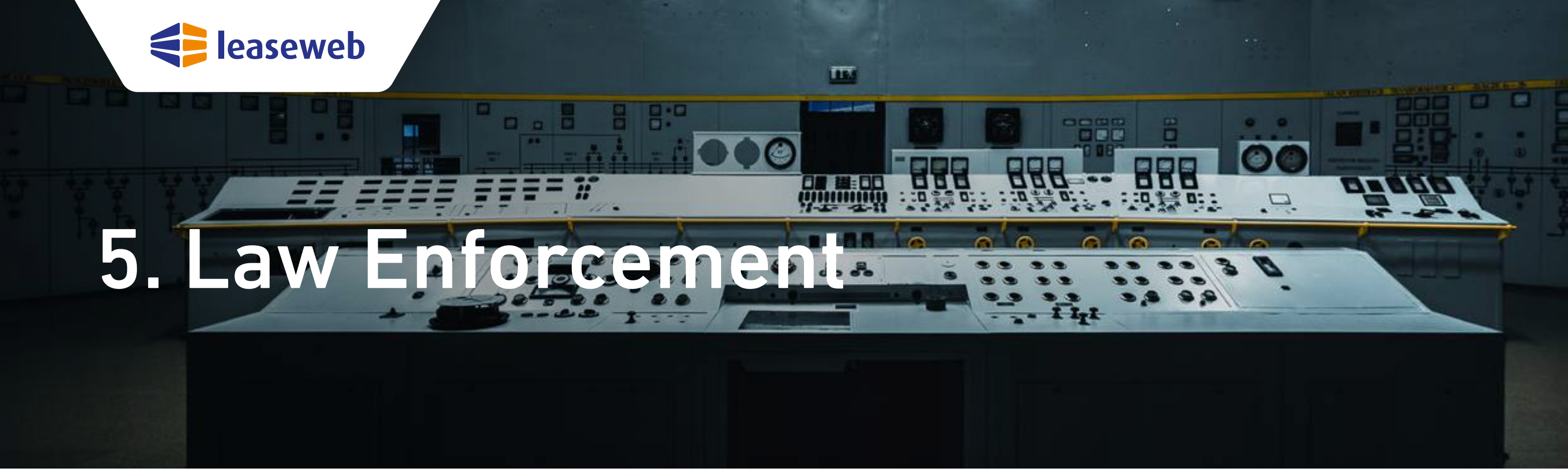
The Compliance department is the gatekeeper of approving new customers, managing the customer verification process, focused on neutral objective KYC control. The purpose of the KYC process is to identify any potentially abusive behavior prior to undergoing contractual agreements, thereby ensuring a healthier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

Benefits of having the KYC process within the Compliance department:

- It quickly identifies abusive and fraudulent ordering behavior because of its automated systems and trained Compliance team
- avoidance of fraudulent ordering and malicious use of services
- Upon termination of a repeating abuse offender, it provides the instant possibility to improve the customer verification process to avoid such new accounts
- Checks and insight in the existence, 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 respecting the swift delivery of the Leaseweb services.

During the verification process extra attention is given to certain types of services such as VPN providers and Cloud Storage Providers ("CSP") due to the potential risk they can bring. Therefore, Leaseweb does her best to filter these businesses during verification and sent out extra verification and questionnaires where the business needs to confirm e.g., they have an abuse policy. Leaseweb has a low tolerance for abuse and does her best effort to minimize the misuse of the Leaseweb network.



5. Law Enforcement

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 possible disclose (under valid orders required by law) the details behind the specific IP address.

Leaseweb Sales Entities take any Law enforcement orders and demands serious, and each request is carefully reviewed by Leaseweb's Compliance team. This team of (legal & compliance) specialists work closely with external law firms and counsels in each jurisdiction of the Leaseweb Sales Entities 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. In addition to advising the Compliance department on law enforcement requests, the law firms also give advice for the Leaseweb Policies and update us if there are regulatory updates, allowing Leaseweb to ensure her work procedures are in line with the applicable laws.
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 provides assistance to the extent in case of such valid orders as 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, one in a certain jurisdiction the legal system generates a high number of orders for law enforcement that are produced and submitted to hosters like Leaseweb, compare to another jurisdiction where the legal grounds for such orders may vary.

Overview of received law enforcement request per Leaseweb Sales Entity

	Leaseweb Netherlands B.V.	Leaseweb Deutschland GmbH.	Leaseweb UK LTD.	Leaseweb Hong Kong LTD.	Leaseweb Asia Pacific Pte. Ltd.	Leaseweb Australia LTD.	Leaseweb USA, INC.
Total	**123**	**353**	**31**	**5**	**37**	**2**	**434**
Accepted	86	274	24	3	29	0	378
Rejected	37	79	7	2	8	2	56

Reasons for rejection can vary from missing data on a request such as timestamps or dates (making it impossible to identify the details the law enforcement agency is requesting), to foreign authorities asking for information without following the route of the mutual legal assistance treaty ("MLAT") to requesting data from a Leaseweb Sales Entity in a different country.

6. Regulatory Matters

Most internet regulated jurisdictions provide safe harbors for hosting providers, to shield them from liability for content that is hosted in 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 regarding 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,[1] 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.

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).

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 ('NTD') procedure. 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[2], 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.

The DSA does not repeal the basic provisions established under the E-Commerce Directive. In fact, it contains identical provisions regarding hosting service providers in its article 5, thus keeping the core of the current conditional intermediary liability regime untouched. However, it does incorporate new regulatory "layers", which may lead to challenging interpretation issues.

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 is no longer passive and may lose the protection offered by the safe harbor, therefor scanning content is 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 cares to demonstrate to regulatory authorities that its role of role of IAAS hosting provider and online intermediary should be defined in a specific manner, with deviation and exemption from any other cloud hosting provider definition.

The legal challenge it to make known that 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

[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

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.

In the TCO regulation all of the above is proposed in the following definition that applies to Leaseweb as 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, and whereby 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 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 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.

6.1 Authority NL – TCO/CSEM

As of June 7, 2022, the TCO regulation comes into place and its set of requirements must be embedded in the Policies of all European platforms and other providers. In the Netherlands the Dutch Authority that will handle the TCO is combined with the Authority to combat CSEM.

TCO requirements:

- Removal of reported terrorist content within 1 hour – 24/7, 365 days a year
- Content is reported from all member states of the EU

These new regulations and requirements will have an impact on Leaseweb Netherlands B.V. and Leaseweb Deutschland GmbH.

6.2 Authority EU

Besides joining forces together on terrorist content, the EU is also preparing a joint effort in combatting child abuse online, named the "Child Sexual Abuse Directive"[3]. The European Commission published in July 2020 the EU Strategy for a more effective fight against child sexual abuse. The Strategy for the period 2020-2025 sets out a comprehensive response to the growing threat of child sexual abuse both offline and online, by improving prevention, investigation, and assistance to victims.

In particular, the Commission committed in the Strategy to:

- propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities[4]

[3] https://ec.europa.eu/home-affairs/Policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_nl

[4] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online/public-consultation_en

7. Focus on removing CSEM (in the Netherlands)

7.1 Leaseweb's Policies anti-CSEM

Leaseweb as Good Hoster believes it is 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. Annually Leaseweb has a constructive meeting with EOKM to support its Good Hoster status.

No doubt that CSEM is prohibited, illegal and strictly banned under the Leaseweb Policies. In Many years ago already, 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, as child erotica does not meet the threshold for legal prohibition in many countries. We believe this contributes to be 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 Entities, where we demand to take the reported abusive content concerning children offline **within 1 hour whereby failure leads to Leaseweb's service interruption to immediately disable the CSEM content.**

Specifically regarding CSEM, Leaseweb identified that this type of abuse is mainly observed in Cloud Storage Providers ('CSP') infrastructures, generated by third party end users uploading this abusive content. Therefore, 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 in itself are lawful and legitimate, they are used for storage and uploading of any material thereby 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 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, over the past 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.

7.2 EOKM HashCheckService Filter

As one of the first Dutch IaaS providers, Leaseweb Netherlands discussed with EOKM ('Expertisebureau Online Kindermisbruik, or "Meldpunt KinderPorno" "KP") to receive the (non-illegal) child erotica abuse notifications to combat such content under the Leaseweb Policies next to 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, used generated image platforms, such as (exploited by) Cloud Storage Providers can implement this HashCheckService, meaning each uploaded file will be

7. Focus on removing CSEM (in the Netherlands)

checked against the abusive collected files in the hash database. If there is a hit, the upload can be blocked.

To jointly stand up against CSEM, Leaseweb works together with the expert desk in the Netherlands (EOKM) as 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 sponsor of EOKM – fully supports the further development and engagement of EOKM with the hosting industry.

The Leaseweb Policies include the mandatory use of this HashCheckService as obligatory part of the Leaseweb Compliance program for its customers -including resellers- such as Cloud Storage Providers and other user generated content websites. Additionally, Leaseweb require its customers to implement and pursue this obligation to use the HashCheckService by their clientele (end users of their user generated services) as mandatory condition of the Leaseweb Policies and the legitimate use of the 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 convinced from its beliefs as 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 to further optimize its Abuse Handling results in regard to CSEM together with EOKM. To illustrate the cooperation between EOKM and Leaseweb, where Leaseweb is presented as a Good Hoster, EOKM provided the following quote:

‘‘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 prevention 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 prevention.

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 nullroute 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. Gerkens, EOKM Director

7. Focus on removing CSEM (in the Netherlands)

7.3 The Focus of the Ministry of Justice and Security.

The Ministry of Justice and Security continues with its focus on the prevention 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 has shown continued effort in the Netherlands to combat CSEM and lead by example in the European Union with this proactive approach. Leaseweb fully embraces and supports this approach, as it has been fully in line with Leaseweb' s Compliance Policies for many years now.

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 advices the Ministry to the need to measure Uptime and make a solid definition of Good Hoster, as opposed to Bad Hoster.

The Ministry will then be enabled to instruct these 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 will keep participating with its Compliance team and management team to embrace these anti-CSEM activities.

leaseweb
reliable hosting

Compliance department - Leaseweb is the brand name under which the various independent Leaseweb entities 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

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