This document sets out the Policies and guidelines applied by Leaseweb in its relationship with Customer, in particular to clarify the manner in which the Services and Equipment may be used by Customer and what manner of use is considered unacceptable by Leaseweb. Leaseweb's Sales Terms and Conditions, Services Specifications, and Service Level Agreement are also part of the Sales Contract and apply to the Services and any Equipment provided by Leaseweb.

CHAPTER A. INTRODUCTION

1. DEFINITIONS

1.1. In addition to the definitions set out in the Sales Terms and Conditions, the Service Level Agreement and the Services Specifications, the following definitions shall apply:

Acceptable Use Policies means Chapter B of these Policies.

Anonymous Proxy means a tool or instrument that accesses the Internet on a user's behalf via a proxy server.

Anonymous Proxy Provider means a business or organization that provides or makes available anonymous proxies as a service.

Authentication Details mean the logins, user identities, passwords, security questions, keys, tokens, URLs and other details that may be used to access the Service.

Blacklist means a so called blacklist or block list which is a basic access control system that denies entry or access to a specific list or range of users or network addresses or IP addresses, as a result of which email sent by a user or from a network address or from an IP address that is on the blacklist will not reach its intended destination or recipient.

CSEM means Child sexual exploitation material including child erotica material. **DDoS** means Distributed-Denial-of-Service.

Deep fakes means the use of an AI system to digitally manipulate (synthetic) audio or visual media capable of generating highly realistic videos or falsely appear to be an existing person.

Digital Services Coordinator means the Digital Services Coordinator as mentioned in the Regulation (EU) 2022/2065 of The European Parliament and Of The Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

DNS means domain name system, which is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

DORA means the EU Digital Resilience Regulation 2022/2254 applicable as of 17 January 2025 to Customers including the ESA delegated act for Regulatory Technical Standards **("RTS")** that are qualified as "Financial Entity" subject to DORA. .

DoS means Denial-of-Service.

DRDoS means Distributed-Reflected-Denial-of-Service.

DSA means the Regulation (EU) 2022/2065 of The European Parliament and Of The Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

Offlimits means the foundation Offlimits (with the Chamber of Commerce number 41217108), incorporated under the laws of the Netherlands, an expertise bureau for combating and prevention of online abuse.

Hit means each individual time a file is sent to the End–User by the CDN Platform.

Hit Factor shall be a fraction, the numerator of which is the number of Hits that have occurred a month, and the denominator is the Utilized Data Traffic for that month measured in GB.

Infrastructure means the Equipment, Service and Instances that support the flow and processing of information, including storage, servers and networking components.

ICANN means Internet Corporation for Assigned Names and Numbers, a not-for-profit public-benefit corporation, which is among other responsible for managing the Internet Protocol address spaces and assignment of address blocks to regional Internet registries, for maintaining registries of Internet protocol identifiers, and for the management of the top-level domain name space.

ICT TPP means ICT third-party service provider under DORA that may be applicable to Leaseweb in case of a Customer that is qualified as Financial Entity under DORA or Customer in its capacity as ICT third-party service provider.

Instant Image Identifier (I3) means a technical tool that transforms any image or video into a hash. This I3 tool allows Customers to check whether files uploaded to their databases are of known CSEM or images for punishable hashes.

IRC means Internet relay chat.

Mail Bomb means (i) e-mailing copies of a single message to many receivers; and/or (ii) sending large or multiple files or messages to a single receiver with malicious intent.

Malicious Software means any type or form of malicious or hostile Software, including but not limited to computer viruses, worms, trojan horses, and spyware (*malware*).

Member State means a member state of European Union.

NOC means Leaseweb's Network Operations Center.

Pentest Audit means the technical security audit performed by the Customer on the Leaseweb infrastructure provided that the technical security activities performed by the Customer fall within the permitted activities as stated in Clause 25 of these Policies.

PTR Record means a pointer record, which is a type of DNS record that resolves an IP address to a domain or host name.

Popular Cached Content means the part of Customer's content that is requested by End-Users in a 48 hour period and is cached on Leaseweb's CDN.

rDNS means reverse DNS, which determines the domain name associated with an IP address. It is used to identify the name of the service provider assigned to an IP address.

RIPE means Réseaux IP Européens, i.e. a collaborative forum open to all parties interested in wide area Internet Protocol networks and the (technical) development of the Internet.

SIDN means the foundation, incorporated under the laws of the Netherlands, for Internet Domain Registration in the Netherlands (Stichting Internet Domeinregistratie Nederland).
Shipment means Customer's own package (including Customer's Equipment) shipped or transported by Customer's carrier to or from the Data Center. Customer is solely liable for its Shipments.
Shipping means any kind of transportation of Customer's Shipment, arranged by Customer's carrier via any type of modalities (air, railway, truck road, and vessel freight forwarding). Customer is solely liable for the Shipping.
Spam means unsolicited bulk messages.
TCO means the terrorist content online as set forth in Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.
TCO Regulation means the Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.
TOR means the onion router, which is software for enabling anonymous communication that routes traffic through multiple anonymizing nodes**.**
TOR Exit Node means the final node that Tor traffic is routed through before it reaches its final destination.
VPN means virtual private network, which is a service that extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
VPN Provider means a business or organization that provides VPN services.
World Wide Web means a system of interlinked documents that runs over the Internet.

2. GENERAL

2.1. Leaseweb aims to promote a high level of responsible behaviour in connection with the use of its Services, as well as, amongst others, the use of the Internet and the use of email. For this purpose, Leaseweb has created these Policies also referred to as Acceptable Use Policies.
2.2. All Customers must comply with the Leaseweb B2B Sales Contract Schedules including these Policies and Customer is required to ensure that its End Users are aware of and comply with the Policies, whereby Customer is fully responsible and accountable for its End Users compliant use of Leaseweb's Services, in addition to such End User individual liability, Customer can be held liable for all its End Users use of the Leaseweb Services. A breach of the Policies by an End User will also be considered a breach of the Policies by Customer.
2.3. Leaseweb is entitled to issue updated versions and thereby amend the Policies. Such amendment applies to existing and new Sales Contracts for all Services, unless Leaseweb states otherwise formally in writing. The amendments come into effect immediately after made available on Leaseweb Website (https://www.leaseweb.com/en/about-us/legal/sales-contract) and are directly applicable for full binding effect, in deviation of Clause 2.3 of the Sales Terms and Conditions.
2.4. At all times, the Customer (and its End Users) shall comply with Leaseweb's KYC requirements to be determined at Leaseweb's sole discretion. This is required in order to ensure the good standing of the Customer, its business, ultimate beneficial owner(s), director(s), shareholder(s) and/or other related staff including compliance with export control restrictions and sanctions as part of Leaseweb's Acceptable Use Policy requirements. In case Leaseweb has reasonable doubts of Customer's good standing of its business and/or related staff and/or is subject to any export control restriction or sanction locally or globally, whatever the source is, Leaseweb is entitled to immediately suspend the Customer and terminate the Sales Contract and cease all Services, without incurring Leaseweb's liability for any costs, expenses and damages as a result of the Customer's (and/or its End Users) non-compliance with Leaseweb's Acceptable Use Policy including Leaseweb's KYC conditions and/or the termination of the Sales Contract and ceasing of Services as notified by Leaseweb to Customer.

3. CONTACT PERSONS

3.1. Customer shall designate (i) contact persons whom Leaseweb may contact at any time in connection with (suspected) violations by Customer or its End Users of the Policies, (ii) contact persons whom Leaseweb may contact at any time in the event of an Emergency.
3.2. Customer will provide to Leaseweb a means of contacting said contact person(s) at any and all times, and Customer shall ensure that the information set out in the Customer Portal with respect these contact persons is and remains up to date.

4. AUTHENTICATION DETAILS

4.1. Some Services may only be accessible through the use of Authentication Details. Customer is solely responsible for the maintenance, security and use of its Authentication Details. All consequences and losses relating to the use of Customer's Authentication Details, whether or not Customer has authorized that use, shall be for Customer's sole account, including all business and communication conducted with Leaseweb through the use of its Authentication Details.
4.2. To the extent possible, Customer shall change its Authentication Details immediately upon receipt thereof by Customer, and Customer shall change the Authentication Details regularly thereafter. Customer will ensure that it will employ best practices when generating Authentication Details.
4.3. If Customer knows or suspects that the security of its Authentication Details has been compromised, or that its Authentication Details are misused, Customer must, as soon as possible, notify Leaseweb and immediately change its Authentication Details.

CHAPTER B. ACCEPTABLE USE POLICY

5. USE OF SERVICES

5.1. Customer represents, warrants and undertakes that it shall (and shall ensure that its End Users shall) only use the Services and Equipment:
a) for lawful purposes; and
b) in accordance with the Sales Contract, the Leaseweb B2B Sales Contract Schedules (consisting of the Sales Terms and Conditions, Policies, Services Specifications, Service Level Agreement) and all applicable laws (within or outside of the Netherlands).

5.2. Without prejudice to the law that applies to the Sales Contract, the Customer acknowledges and agrees that the Customer's use –and its End User's use of the Services and Equipment is to be compliant with (mandatory) law of the Netherlands, as well as with other laws applicable to Customers or its use of the Services and Equipment.

5.3. Customer shall refrain from any use of the Services and Equipment which may have an adverse effect on Leaseweb's good name or standing, or may cause damage to Leaseweb's business operations, or may subject Leaseweb to litigation, or may cause Leaseweb to be in breach of applicable laws.

5.4. Leaseweb prohibits the use of the Services and Equipment by Customer, End User or any other third parties for certain activites (such as hosting, storing, distributing, processing or otherwise making available), content and materials for the purposes of or relating to: (i) terrorism and/or dissemination to the public of terrorist content online TCO; (ii) threatening harm to persons or property or otherwise harassing behaviour; (iii) violating local export control laws for Software or technical information; (iv) the use or transmission, reproduction or distribution of any data or material that infringes any Intellectual Property Rights; (v) the manufacture or use or distribution of counterfeit, pirated or illegal software or other product; (vi) providing or offering compensation to End Users based on download volume, unless Customer knows – or has no reason to doubt – that such End Users are using Customer's services only for lawful purposes and for the distribution or dissemination of their own data or material, or of data or materials for which they have the proper authorisation to distribute or disseminate the same; (vii) fraudulently representing products or services; (viii) uploading, storing, distributing or otherwise making available any content or materials that are prohibited or illegal in any relevant jurisdiction, including any defamatory materials or any obscene materials that contain, zoophilia, child pornography and virtual child pornography, and child erotica; (ix) illegal content and disinformation and illegal deep fakes; (xi) compromising the security (or tampering with) system resources or accounts of other Customers or of any other Internet sites or intranet sites without the proper authorisation; (xii) Spamming, phishing, DoS attacks, DDoS attacks, DRDoS attacks without proper authorisation; xiii) intentionally accessing a computer system or Infrastructure structure component without authorization or exceeding authorized access levels thereof; (xiv) activities that may result in the placement or inclusion on a Blacklist of Customer, Customer's IP address(es) and/or IP address(es) assigned by Leaseweb to Customer; (xv) non-authorized scans and/or penetration testing and (xvi) facilitating, aiding, or encouraging any of the foregoing activities. Customer shall not (and shall ensure that its End Users shall not) use the Services for or in relation to any such prohibited activities.

5.5. Customer acknowledges that any use by Customer and/or its End Users of the Services in breach of the Acceptable Use Policy could subject Customer and/or its End Users to criminal and/or civil liability, in addition to other actions by Leaseweb outlined in Chapter H of the Policies and in the Sales Terms and Conditions.

5.6. Customer, and (in accordance with U.S. Affiliates Rule) on behalf of its ultimate beneficial owner(s), affiliate(s), branch(es), End-User(s) and its resident(s) in a certain country for which Customer will be held responsible and liable ("**Customer CS**") agrees to:

a) not to order, buy, use, (re)sell, (sub)license, export, re-export and/or transfer (in-country) in any way the following Services configurated with regulated GPUs (chips) from Leaseweb. Regulated GPUs mean the product, including hardware software and technology in any way directly or indirectly in breach of U.S. export control laws subject to U.S. Export Administration Regulations ("**EAR**") or any other related Bureau of Industry and Security ("**BIS**") rules listed as L4, L40, L40S, H100, H200, A100.

b) to not be directly and/or indirectly located in, and/or organized under the laws of specified countries referred to as Country Group D:1, D:4, D:5 and E (where by Hong Kong is included as part of China): Afghanistan, Armenia, Azerbaijan, Bahrein, Belarus, Burma, Cambodia, Central African Republic, China including Hong Kong, Democratic Republic of Congo, Cuba, Egypt, Eritrea, Georgia, Haiti, Iran, Iraq, Israel, Jordan, Kazakhstan, North Korea, Kyrgyzstan, Kuwait, Laos, Lebanon, Libya, Macau, Moldova, Mongolia, Nicaragua, Oman, Pakistan, Qatar, Russia, Saudi Arabia, Somalia, Republic of South Sudan, Sudan, Syria, Tajikistan, Turkmenistan, United Arab Emirates, Uzbekistan, Venezuela, Vietnam, Yemen, Zimbabwe as referred in the EAR Supplement No. 1 to Part 740 and any updates thereof ("**Prohibited Countries**").

c) Not to be qualified as military-End-User, and/or government End-Users (Part 772 EAR), or End-User of the Services for military purposes, including weapons of mass destruction ("**Prohibited Segments**").

d) not to order, buy, use, (re)sell, (sub)license, export, re-export and/or transfer (in-country) the Service in any way not use the Services for advanced computing integrated circuits (ICs) or similar functionality for development of semiconductors or supercomputers in abovementioned Prohibited Countries (Part 744 EAR).

5.7. In accordance with the applicable dual-use export control regulations, the Services shall only be used for civilian purposes, Customer CS warrants that it will not use the Services for military purpose, weapons of mass destruction, excluding any military-End-User(s), or government End-User(s) .

5.8. In accordance with the Affiliates Rule, Customer CS shall be subject to sanctions regimes of EU, the U.S. Department of Treasure Office of Foreign Asset Controls ("**OFAC**") including the Specially Designated Nationals List which contains the names of restricted individuals, entities and groups designated by OFAC, and shall be subject of Leaseweb's and Customer CS's own jurisdiction.

5.9. These Customer CS obligations are subject to the Customer Warranties of the Leaseweb Sales Terms and Conditions, as well as the KYC provisions in Clause 2 of the Policies and Leaseweb's rights and remedies for suspension and termination set out in the Leaseweb Sales Terms and Conditions.

5.10. License terms on regulated and/or non-regulated GPUs applicable to the Customer are set out in Clauses 40.6 – 40.9 of the Services Specifications.

5.11. Leaseweb maintains a Restricted Business Policy under which the sale, delivery or use of Leaseweb's services to Customer CS in or to the following jurisdictions is prohibited: Cuba, Iran, North-Korea, Syria, Russia, Belarus, Sudan, Myanmar, Venezuela, occupied regions of Ukraine (Crimea, Donetsk and Luhansk), in addition Leaseweb may restrict its services to what it deems to be high-risk countries ("Restricted Business"). Leaseweb reserves the right to reject, suspend or cancel any order or terminate any Sales Contract that directly or indirectly involves any of such Restricted Business.

6. ELECTRONIC MESSAGES / ANTI-SPAM

6.1. Customer may not (i) send electronic messages that in any way is or may be in breach of applicable law; (ii) send or propagate Spam and shall not allow its End Users or third parties to send or propagate Spam via Customer's IP addresses; (iii) send, propagate, or reply to Mail Bombs

and shall not allow its End Users or third parties to send or propagate Mail Bombs via Customer's IP addresses; or (iv) alter the headers of electronic messages to conceal Customer's address or to prevent receivers from responding to messages.

6.2. Customer shall refrain from any activities that may result in the placement of Customer or Customer's IP address(es) on a Blacklist. Leaseweb reserves the right to charge Customer the Express Delisting Fees as stipulated on the UCEProtect website for Level 2 Listing of a Leaseweb's IP range(s) and/or Level 3 Listing of Leaseweb's ASN or three hundred Euros (€ 300,--) per hour in consulting Fees for any remedial actions that Leaseweb elects to take in the event that, as a result of Customer's activities or Customer's end-user(s), Leaseweb's servers or IP address(es) are placed in any third-party filtering software or Blacklist or the Leaseweb's IP range(s) and/or ASN are placed on the UCEProtect Blacklist.

6.3. Bulk messages are only permitted if (i) the Customer has obtained the explicit consent from each of the recipients via double opt-in, and/or (ii) applicable law permits the sending of such messages without the recipients' consent. Customer is obliged to offer in each electronic message, an easily accessible functioning unsubscribe mechanism, and Customer shall immediately cease sending electronic messages to a recipient after the recipient has unsubscribed.

7. INTERNET USE

7.1. Customer is prohibited from posting or transmitting unlawful material on or via the Internet or the World Wide Web.

7.2. Leaseweb is entitled to actively block ports or IP addresses for the Network, in the event that such is – in Leaseweb's reasonable view – necessary to preserve or protect the security and performance of the Network or the Internet or the World Wide Web. An overview of the blocked ports or IP addresses may be requested in writing by Customer from Leaseweb.

7.3. Without prejudice to the generality of Clause 7.2 of the Acceptable Use Policy, Leaseweb shall in any event actively block the following ports for its Network: (i) UDP/137 – Netbios; (ii) UDP/139 – Netbios; (iii) TCP/135 till 139 – Netbios;(iv) TCP/445 – Smb; and (v) Protocol UDP port 11211 – Memcache.

7.4. If Leaseweb reasonably suspects that Customer is subject to a DoS attack, DDoS attack, DRDoS attack or another attack and (in Leaseweb's reasonable opinion) such attack negatively affects the Infrastructure, Leaseweb shall be entitled to immediately block access to Customer's Infrastructure. In the event that Customer is subject to repetitive attacks, and Customer does not successfully take measures to prevent that future attacks may negatively affect Leaseweb's Infrastructure, then Leaseweb shall be entitled to immediately terminate theSales Contract by sending a written notice to Customer.

8. IRC USE

8.1. Customer is prohibited from posting or transmitting inappropriate material via the use of IRC or to otherwise use IRC in a manner that is in breach of the Acceptable Use Policy. For the purpose of this clause, prohibited use of IRC include so called 'eggdrops' and 'psybnc shell hosting'.

8.2. Without the prior written consent of Leaseweb, which Leaseweb may grant or deny in its sole and absolute discretion, Customer is prohibited from hosting an IRC server, regardless of whether it concerns a stand-alone IRC server or an IRC server that connects to global IRC networks.

9. USE OF THE CUSTOMER PORTAL

9.1. Subject to the terms of use applied from time to time by Leaseweb Global B.V., and subject to the provisions of the Sales Contract, and Customer's compliance therewith, Leaseweb shall arrange that Leaseweb Global B.V. will grant a non-exclusive, non-transferable, non-assignable, non-sublicensable and royalty free right to use the Customer Portal during the Term. Use of the Customer Portal by or on behalf of Customer shall be at Customer's risk and responsibility.

9.2. Customer shall observe each and any instruction of Leaseweb Global B.V. regarding the use of the Customer Portal.

10. USE AND REGISTRATION OF (INTERNET) DOMAINS/IP ADDRESSES/AS NUMBERS

10.1. Customer shall comply with the policies, guidelines, terms and conditions applied from time to time by the organization or entity which is responsible for the management (registration and/or distribution and/or giving into use) of an (Internet) domain, such as – for example – ICANN.

10.2. Customer shall comply with the policies, guidelines, terms and conditions applied from time to time by the organization or entity which is responsible for the management (registration and/or distribution and/or giving into use) of IP addresses and AS numbers, i.e. the regional Internet registries of RIPE.

11. RESTRICTIONS ON USE OF SHARED WEB HOSTING SERVICES

11.1. Customer may not:

a) use the Shared Web Hosting Services in a manner that may interfere with or otherwise disrupt services to other customers of Leaseweb or Leaseweb's infrastructure or that may cause an Emergency;
b) knowingly allow any other website or hosting server to link to content stored on Leaseweb's systems. At least 75% of any content stored on Leaseweb's systems must have associated HTML, PHP or similar files at the Shared Web Hosting Service linking to the content stored on the Shared Web Hosting Services;
c) exceed the Shared Web Hosting Services limits, such as allotted diskspace or bandwidth;
d) run scheduled tasks, such as cron entries, with intervals of less than fifteen (15) minutes;
e) run stand-alone, unattached server side processes or deamons on the Shared Web Hosting Platform;
f) send more than 3 emails per minute/180 emails per hour; and/or
g) use Shared Web Hosting Services for hosting Mailer Pro, Push button mail scripts, proxy scripts/anonymizers, autoSurf/PTC/PTS/PPC sites, spiders, crawlers, indexers, banner-ad services (commercial banner ad rotation).

11.2. If Leaseweb detects failed login attempts to the Shared Web Hosting Service, it may, without notice and without obligations of any kind, ban network access from the source of those failed attempts.

CHAPTER C. ABUSE COMPLIANCE POLICY

12. ILLEGAL CONTENT AND ABUSE HANDLING

12.1. In connection with use of the Services, Customer shall adopt and apply an abuse handling procedure which is compliant with the Policies, with the law that applies to the Sales Contract and with any other law applicable to Customer, including the DSA.

12.2. Customer shall log (date and timestamp) each Abuse Notification (as defined below) received by Customer from Leaseweb and from third parties, including the nature of the notification (e.g. copyright infringement), as well as Customer's response to such complaint, and the moment that Customer deems the Abuse Notification to be resolved.

12.3. Customer shall maintain the log in respect of each Abuse Notification for a minimum of two (2) years after the date that Customer deems such Abuse Notification to be resolved. Customer will provide Leaseweb with a copy of its Abuse Notification log, upon Leaseweb's request.

12.4. Customer shall ensure the availability of sufficient and properly trained personnel to ensure that Customer's End Users comply with the Policies and to apply Customer's abuse handling procedure and to handle the volume of abuse notifications that arrive without backlogs.

12.5. In order to prevent any breach of Clause 5.4 of the Policies, the Customer shall fulfill its obligation on behalf of its End Users to demonstrate and timely execute its fully compliant proper performance of these Policies.

12.6. If a Customer is a VPN Provider or Anonymous Proxy Provider, Customer shall be obliged to comply with the following requirements in connection with the use of the Services:

a) Customer's company information must be visible and available on its website (including a publicly available email address for abuse handling purposes and copyright-related complaints),
b) Customer shall enter into a user-agreement with its End Users that shall include provisions to ensure an End User's compliance with applicable law, including but not limited to intellectual property law, and with the Policies,
c) Customer shall maintain accurate rDNS/PTR records containing Customer identifying information for all IP addresses that are used by Customer and/or its End Users to provide VPN / Anonymous Proxy services,
d) when requested by Leaseweb at Leaseweb's sole discretion, Customer shall provide the relevant information required for Leaseweb to update Leaseweb rWHOIS records with the correspondent regional IP address registry, within a reasonable time as indicated in the request,
e) Customer shall comply with the repeat infringer policy in Section 14,
f) Customer shall implement and apply reasonable measures to prevent an End User -that has been terminated for repeat-infringement- from recommencing the use of Customer's services or the use of the Services through or via Customer,
g) Customer shall implement and apply technical measures designed to inhibit non-compliant or infringing activities.

12.7. If a Customer is a Tor-Exit node Operator, Customer shall be obliged to comply with the following requirements in connection with the use of the Services: (i) Customer shall in any event actively close/block such ports that are generally known to be used or are generally associated with non-compliant or infringing activities, a list of which may from time to time be published by Leaseweb or provided to Customers, (ii) Customer's rDNS records shall start with 'tor.exit.node.', (iii) Customer shall add a working email address to the 'torrc' file to allow for direct contact with Customer if required by End Users or third parties.

12.8. In connection with the use of the Services, Customer shall be obligated and is responsible for the pro-active initiatives for purposes of technical adoption, contractual engagement and active use of the Instant Image Identifier (I3) operated by Offlimits for any user generated content websites in order to fully prevent any abuse of illegal content and non-compliant use of the Service in breach of Clause 5.4 of the Fair Use Terms, thereby fulfilling Customer's obligation on behalf of its End Users to demonstrate its full compliance. In addition, if Customer is notified by the Compliance department to undertake this responsibility, Customer shall be obliged to report to Offlimits within twenty-four (24) hours to sign the agreement for acceptance and implementation of the Instant Image Identifier (I3) guaranteeing towards Offlimits and Leaseweb the active use thereof. This obligation is deemed a guaranteed performance by Customer also for and on behalf of its End Users for whom the Customer shall be held responsible and liable. The obligation by Customer for the Offlimits engagement and active use of the Instant Image Identifier (I3) is part of Leaseweb's continuous zero tolerance approach towards any CSEM content notified and/or found within its network. If Customers fails to comply with the Policies to prevent CSEM and Child erotica in accordance with this continued zero tolerance approach and/or fails to fully and adequately remove such content within the deadlines notified by Leaseweb, Leaseweb is entitled - for each of such failure or alleged circumstances to expect such failure - to disable and suspend the Services by means of null routing and terminate the Services.

12.9. Customer acknowledges that a failure to comply with Clause 12.8 by Customer and/or its End Users of the Services shall result in an immediate material breach of the Acceptable Use Policy without any requirement of Leaseweb's further notifications. Leaseweb is entitled at its full discretion to immediately suspend and/or terminate the Services and Sales Contract without Leaseweb incurring any liability for such termination or any damages and costs resulting thereof while the Customer shall keep Leaseweb fully indemnified for any damages including reputation and immaterial, indirect and consequential damages and will keep Leaseweb harmless for any third-party claims.

12.10. In connection with the use of the Services, Customer shall be obligated and is responsible for the satisfactory pro-active initiatives on behalf of itself and its End Users to fully prevent dissemination of terrorist content online by making use of the Services.

a) In order to fully prevent any dissemination of TCO and breach of Clause 5.4 of the Leaseweb Policies, the Customer shall fulfill its obligation on behalf of its End Users to demonstrate and timely execute its fully compliant proper performance of these Policies, based on the TCO Regulation and instructions from a national competent authority.
b) If Customer is notified by the Leaseweb Compliance department and/or a national competent authority to undertake this Customer responsibility on behalf of itself and its End Users, Customer shall be obliged to timely remove reported prohibited content within one (1) hour, in accordance with the TCO. This obligation is deemed a Customer warranty for and on behalf of its End Users for whom the Customer shall be held responsible and liable to represent and undertake its compliance with the TCO and to indemnify and keep Leaseweb harmless.
c) If Customers fails to comply with the Policies and/or instructions from a national competent authority to prevent such prohibited content in accordance with the TCO Regulation and/or fails to fully and adequately remove such content within the deadlines notified by Leaseweb and set forth in the TCO Regulation, Leaseweb applies its zero tolerance approach, Leaseweb is entitled - for each of such failure or alleged circumstances to expect such failure - to disable and suspend the Services by means of null routing and terminate the Services.

13. ABUSE AND ILLEGAL CONTENT PROCEDURE

13.1. Leaseweb has an Abuse and illegal content Procedure ("**Abuse Procedure")** which is set out on https://www.leaseweb.com/abuse-handling. This gives third parties the option to notify ("**Notifier**") Leaseweb by e-mail of (alleged) illegal content and abusive material that is accessible via its Services.

13.2. If Leaseweb is notified by a Notifier (including any law enforcement authority) of a (suspected) violation by Customer and/or the End-User of the Acceptable Use Policy and/or any applicable law (an "**Abuse Notification**"), Leaseweb shall notify Customer hereof by way of email or such other method of communication as Leaseweb deems appropriate and in accordance with the DSA.

13.3. Customer shall, within the response period or remedy period set forth in Leaseweb's notification (the "**Remedy Period**"), take remedial action to cure the violation and within the Remedy Period inform Leaseweb of the actions taken by Customer.

13.4. In some cases, Leaseweb may grant the Customer the option to contest the alleged violation by filing a counter notice (a "**Counter Notice**"). If Customer chooses to file a Counter Notice, Customer must use the online form made available to Customer for this purpose. Leaseweb shall review the submitted information and may (in Leaseweb's sole discretion) decide to reject Customer's Counter Notice, and require Customer to take immediate remedial action, if – in Leaseweb's sole discretion – Customer's or the End-User's content or actions are unmistakably unlawful and/or may subject Leaseweb to third party claims and/or litigation.

13.5. If Leaseweb does not reject Customer's Counter Notice, Customer shall – upon Leaseweb's request – provide a deposit or a bank guarantee or a parent guarantee or other security satisfactory to Leaseweb. The amount of the security will be determined by Leaseweb at its sole discretion. The security is intended to cover Customer's obligations, and any claim of Leaseweb, under the indemnity specified in the Sales Terms and Conditions. Furthermore, in the event that Customer files a Counter Notice, Customer shall within two (2) days of its response to Leaseweb notify Leaseweb whether an attorney will be representing Customer and, if so, which attorney.

13.6. Customer shall provide Leaseweb with all documents and information in connection with the Abuse Notification without cost and on first demand.

13.7. As a condition to the (continued) provision of Services and/or to resuming the provision of Services, Leaseweb shall be entitled to require Customer: (i) to execute a cease-and-desist declaration; and/or - as appropriate - (ii) to confirm in writing that Customer's End User who was responsible for the violation, has been permanently excluded from using the Service.

13.8. If Customer does not respond (in a timely manner) to an Abuse Notification that Leaseweb has forwarded to the Customer, or if Customer does not take the necessary remedial measures (in a timely manner) or does not follow up a notification in a timely manner within the set deadline, Leaseweb shall take measures against the Customer in order to prevent further violations of applicable law and the Leaseweb Policies.

14. STATEMENT OF REASONS

14.1. If Leaseweb has taken an action that has restricted the Services in accordance with the DSA, it will provide a clear and specific statement of reasons to affected Customer of the Service for any of the following restrictions imposed on the ground that the information provided by the Customer of the Service is illegal content or incompatible with the Policies or applicable laws. This shall not apply where the information is deceptive high-volume commercial content (SPAM).

14.2. Leaseweb shall act in a diligent, objective, and proportionate manner in applying and enforcing the restrictions, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the Customer, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights.

14.3. The statement of reasons shall be given no later than the date on which the restriction is imposed, irrespective of why or how it was imposed.

14.4. The statement of reasons shall contain at least the following information (i) the facts and circumstances on which the decision is based, including, where appropriate, whether the decision was taken as a result of a notification made under Article 16 DSA; (ii) if the decision is based on the alleged incompatibility of the information with Leaseweb's Sales Terms and Conditions and/or Policies, a reference to the relevant contractual provision and an explanation of why the information is considered incompatible with it.

14.5. If Customer objects to any measures Leaseweb has taken, whether it is after a notice, or following other information, Customer can send a detailed response (with all documents and information in connection with the Abuse Notification) with motivation to dsa@global.leaseweb.com within six months after the date Leaseweb has taken action, provided the Sales Contract has not been cancelled or terminated within this time frame. Leaseweb will then decide within a reasonable period whether the taken measures were justified, or that another action should be taken.

14.6. If the Customer is not satisfied with the results of the internal compliant-handling mechanism as stated in the previous clause, then Customer reserves the right to initiate legal proceedings against the statement of reasons with the before the competent court under applicable law.

15. REPEAT INFRINGERS AND LIVE VIDEO STREAMS

15.1. As part of its abuse handling procedure, Customer should make reasonable efforts to detect repeated attempts by its End Users to store, transfer, or distribute - on or through Customer's services - (i) materials or data which violate or infringe the Acceptable Use Policies; or (ii) that Customer previously deleted or disabled following receipt of an Abuse Notification.

15.2. Customer shall immediately terminate the provision of service to an End User -and terminate an End User's access to the Services, in the event that such End User is discovered to be a repeat infringer or violator of the Leaseweb Policies.

15.3. Customer shall, upon request, demonstrate compliance with the following requirements:

a) Confirm it has established and implemented its own repeat infringer policy;
b) Publish a publicly available statement or policy prohibiting use of its services to infringe copyright;
c) Publicly designate a copyright abuse agent (including a publicly available email address).

15.4. In the event Customer's services are repeatedly used for streaming of live video and/or audio, Customer shall offer an online take down tool to trusted third parties (or their agents) to allow them to immediately terminate live video streams which are infringing on the intellectual property rights of these trusted third parties.

CHAPTER D. FAIR USE POLICY

16. IP CONNECTIVITY

16.1. The IP Connectivity Service is provided for Customer's consistent, fair, and reasonable use.

16.2. Customer's use of IP Connectivity shall be deemed unfair and unreasonable, if Leaseweb determines (in its sole discretion) that Customer's actual or projected use of IP Connectivity exceeds, or is likely to exceed, the monthly Committed Bandwidth or Committed Data Traffic by more than 100%, and such use affects the provision of services by Leaseweb to other Leaseweb customers. If the Customer has not agreed to Committed Bandwidth or Committed Data Traffic, then for the purpose of interpreting this clause 16.2 only, the Committed Bandwidth or Committed Data Traffic (as applicable) shall be deemed the lowest value of the Committed Bandwidth or Committed Data Traffic offered by Leaseweb for the respective Service.

16.3. Customer's use of IP Connectivity is deemed to be inconsistent, if Customer's use thereof results in irregular Bandwidth or Data Traffic usage patterns, either on a per server basis or as part of a group of Customer's servers/Instances.

16.4. Should Customer's Traffic pattern result in an ASN Destination Percentage for a certain ASN number higher than the percentages below (the "**ASN Threshold**"), then the Data Traffic or Bandwidth in excess of the ASN Threshold shall be charged at EUR 3,00 (three euro) per TB or EUR 0,75 (seventy-five euro-cents) per Mbps on top of the contracted rate.

Table 1: ASN Thresholds

ASN DESTINATION	REGION	ASN THRESHOLD
AS701 (Verizon)	US	10%
7922 (Comcast)	US	10%,
20115 (Charter)	US	10%
7018 (AT&T)	US	10%
AS9121 (Turktelecom)	EU	10%
AS3320 (DTAG)	EU	5%
AS3352 (Telefonica)	EU	10%
AS3215 (Orange)	EU	10%

17. DEDICATED EQUIPMENT

17.1. Dedicated Equipment is provided to Customer in private racks and shared racks. To protect the performance and integrity of the racks, Customer shall in respect of all Dedicated Equipment ensure that its consumption of electricity, network and the use of Dedicated Equipment resources including but not limited to storage devices, shall be fair and reasonable.

17.2. Customer's consumption of electricity, network and Dedicated Equipment resources shall be deemed not fair and not reasonable, if Customer's use exceeds the Basic Power (as agreed in the Contract Overview) or exceeds the intended use of network and Dedicated Equipment resources including storage devices in such a way that at Leaseweb's sole discretion it may affect the use of other Leaseweb's Customer in the shared rack and performance of other Infrastructure in the racks, or exceed the intended use of Dedicated Equipment resources thereby greatly reducing its lifetime.

17.3. Dedicated Equipment in shared racks, is provided to Customer in a rack shared with other Leaseweb's Customers and therefore Customer's consumption of electricity exceeding the Basic Power may affect the performance such as latency, bandwidth and/or IOPS of the Dedicated Equipment in the shared racks. To protect the performance and integrity of the Dedicated Equipment, Customer shall ensure that its consumption of electricity, network and Dedicated Equipment resources shall be fair and reasonable.

18. CLOUD SERVICES

18.1. Compute Capacity of the Cloud Platform for the Public Cloud Services is provided to Customer on a shared basis. To protect the performance and integrity of the Cloud Platform, Customer shall, in respect of Public Cloud Service, ensure that its use of Compute Capacity shall be fair and reasonable.

18.2. Customer's use of Compute Capacity shall be automatically deemed not fair and not reasonable, if Customer's use exceeds Leaseweb's overbooking factor as determined in the Service Specifications in such a way that at Leaseweb's sole discretion it may affect the performance of other Infrastructure on the Cloud Platform.

19. VPS SERVICE FAIR USE

19.1. Compute Capacity of the Cloud environment for the VPS Services is provided to Customer on a shared basis with other customers of Leaseweb. In order to protect the performance and integrity of the Cloud environment Customer shall, in respect of VPS Service, ensure that its use of Compute Capacity shall be fair and reasonable.

19.2. Customer's use of compute capacity shall be considered unfair and unreasonable if the Customer utilizes the allocated compute capacity continuously exceeding reasonable usage of the shared environment. The Customer is using the shared environment in an unreasonable way if, in Leaseweb's sole discretion, it leads to the continuous high use of CPU usage and Service issues such as, but not limited to, CPU steal. In case a user exceeds fair usage, Leaseweb may apply CPU limitations to ensure equitable resource distribution.

19.3. Customer's use of bandwidth capacity shall be deemed unfair and unreasonable if the Customer continuously uses high amounts of data traffic leading to service issues with the VPS Service determined in Leaseweb's sole discretion. By adhering to this policy, Leaseweb can ensure that the shared network infrastructure performs optimally for the Customer. In case a user exceeds fair usage, Leaseweb may limit the use of data-traffic or suspend the use of the service.

20. CLOUD STORAGE SERVICES

20.1. Leaseweb offers Cloud Storage Services, a Cloud Storage components of the Cloud Platform ("**Cloud Storage Services**"), with different storage types, storage capacity and performance tiers, differentiated on IOPS per volume and latency assigned to each tier. The Cloud Storage Services are provided to Customer on a shared storage system, and therefore Customer's use of the Cloud Storage Services may affect the performance (such as latency, storage bandwidth and IOPS) of the storage system as a whole. The IOPS per volume are based on a usage profile of 4K block size with 70/30 read/write use ("**Usage Profile**"), by default.

20.2. To protect the performance and integrity of the Cloud Platform, Customer shall ensure that its use of the Cloud Storage Service shall be fair and reasonable in line with its Usage Profile. Other Usage Profiles are supported by Leaseweb, but they may lead to different IOPS performance results.

20.3. Customer's use of the Cloud Storage Services shall be deemed unfair and unreasonable, if the Cloud Platform usage is consistently deviating from the Usage Profile in such a way that it affects the performance of the Cloud Platform as a whole, to be solely determined by Leaseweb at its sole discretion based on its own information and tools. Consistent deviating use that is deemed to be unfair and unreasonable will result in additional Fees.

21. SHARED WEB HOSTING SERVICE

21.1. Leaseweb's Shared Web Hosting Platform is made available to Customer on a shared basis. To protect the performance and integrity of the Leaseweb Shared Web Hosting Platform, Customer shall ensure that its use of Shared Web Hosting Services shall be fair and reasonable.

21.2. Customer's use of the Shared Web Hosting Services shall be deemed unfair and unreasonable, if:

a) Customer uses the Shared Web Hosting Services in such a way that (in Leaseweb's reasonable opinion) it affects the performance of the Shared Web Hosting Platform or causes an Emergency;
b) the database size exceeds the total disk space allotted to Customer on the Shared Web Hosting Platform by 30%;
c) IMAP exceeds 5 connections per IP address;
d) twenty-five percent (25%) or more of the system resources are used in connection with Shared Web Hosting Services for longer than ninety (90) seconds at a time. Activities that could cause this excessive use include, but are not limited to, CGI scripts, FTP, PHP, HTTP; and/or
e) Customer runs any MySQL queries longer than twenty (20) seconds. MySQL tables should be indexed appropriately.

22. MULTI-CDN

22.1. The Multi-CDN Service is provided for Customer's consistent, fair and reasonable use.

22.2. Data Traffic Limits: Leaseweb reserves the right to limit the amount of Leaseweb Shield CDN Data Traffic passed through the Leaseweb Shield CDN to ensure the stability and reliability of our Network. If a Customer's Shield CDN Data Traffic exceeds 5% of the Monthly Committed Data Traffic, Leaseweb may (i) limit Customer's Leaseweb Shield CDN Traffic, (ii) purge the cache on Leaseweb Shield CDN and/or (iii) disable Customer's Leaseweb Shield CDN setup to prevent disruption of other Customers' Multi-CDN Services.

22.3. Object size: Customer agrees and acknowledges that the Multi-CDN Services Fees are based upon an average object delivery size of 32KB or larger per HTTP/HTTPS request. Leaseweb reserves the right to charge Customer an additional Fee per 10.000 HTTP/HTTPS requests for Data Traffic with an average object of less than a 32KB.

22.4. The usage of the Leaseweb Shield CDN by Customer as a storage service is strictly prohibited.

22.5. The usage of the Multi-CDN Service by Customer shall be deemed inconsistent, unfair and/or unreasonable in the event (i) Customer exceeds the Leaseweb Shield CDN Traffic limits in Clause 15.2, or (ii) Customer's average object size is less than 32KB, and/or (iii) the Leaseweb Shield CDN is being used as a storage service.

22.6. In the event Leaseweb determines in its sole discretion, that Customer is not using the Multi-CDN Service in accordance with this Multi-CDN Fair Use Policy, Leaseweb shall be entitled to immediately impose limits on of the Data Traffic the Customer may transmit/receive through the Multi-CDN Service without any prior notice and Leaseweb shall be entitled to terminate the Multi-CDN Services.

CHAPTER E. SECURITY POLICY

23. INFRASTRUCTURE CONFIGURATION

23.1. Leaseweb promotes a high level of responsible behavior in connection with the use of Leaseweb services and requires that users of Leaseweb Services do the same. For this reason, Leaseweb has established information security requirements for all Leaseweb Services, including standards for the basic configuration of Infrastructure, the use of Authentication Details and the use of effective Malicious Software detection and prevention.

23.2. Customer is advised (i) to back-up (critical) data and system configurations on a regular basis and store such data in a safe place, and (ii) not to connect its Infrastructure via a wireless connection, (iii) to keep the Software operated or used on the Infrastructure up to date, and accordingly to install updates and patches on a regular basis without undue delay after becoming available, (iv) to operate and/or use adequate measures against Malicious Software on the Infrastructure.

23.3. Customer shall ensure that all data distributed through the Service shall be free of Viruses. Leaseweb may, without giving any notice and without incurring any liability vis-à-vis Customer, (temporarily) suspend or (temporarily) disconnect from the Network, any Service found to be infected with a Virus. The suspension shall continue until the Virus has been removed and the infection has been cured.

24. MONITORING / REPORTING

24.1. Customer shall implement logging and monitoring measures for security-related events.

24.2. Customer shall immediately report to Leaseweb's NOC any security-related event that may materially impact Leaseweb's Infrastructure, Leaseweb's organization or Leaseweb's provision of services to other customers. Customer shall make the log in relation to such event

immediately available to Leaseweb upon Leaseweb's request, and shall follow any directions given by Leaseweb's as may be required to contain or correct the event.

25. PENTEST AUDIT

25.1. Customer is allowed to perform a certain Pentest Audit on Leaseweb's Equipment provided that the conditions set out in this Clause 25 are met. The number of Pentest Audit allowed shall be limited to a maximum of one time per month.

25.2. Permitted activities under a Pentest Audit include (i) testing of Customer's web applications, (ii) vulnerability scanning, (iii) fuzz testing of the Services, (iv) port scanning of the Services, (v) PCI-DSS compliance testing, (vi) testing of Customer's security monitoring and detections.

25.3. Prohibited activities under a Pentest Audit include but are not limited to the followings: (i) tests on other Customers' Services, (ii) direct tests on shared network infrastructure, (iii) tests on shared virtual infrastructure, (iv) tests on shared webhosting, (v) DoS tests, (vi) phishing or other social engineering attacks against Leaseweb employees.

25.4. Customer shall bear all the costs related to the Pentest Audit. Customer shall be solely liable for its auditor's activities towards Leaseweb and third parties. When performing the audit, the Customer's auditor shall act responsibly, with due diligence and observe a duty of care with respect to Leaseweb and its business. Customer's auditor will under no circumstances perform activities that are generally known or suspected to cause damage to the Service provided by Leaseweb and its Customers, or an interruption, suspension or degradation in the provision of one or more Services provided by Leaseweb to its Customers.

25.5. Customer shall (i) indemnify and hold Leaseweb harmless against all actions, losses, costs, damages, awards, expenses, fees (including legal fees incurred and/or awarded against Leaseweb), proceedings, claims or demands due to tests performed by the Customer's auditor, (ii) provide, at the Customer's sole expense, Leaseweb with full authority, information and assistance as is reasonably necessary for the defense, compromise or settlement of such claim; and (iii) at the request of Leaseweb, take those steps that are reasonably required to put Leaseweb in the financial position it would have been in if the test(s) by the Customer's auditor had not occurred.

25.6. If during the Pentest Audit Leaseweb's Equipment and/or environment becomes unstable, the Customer's auditor shall be obligated to immediately stop all auditing activities and contact Leaseweb at support@leaseweb.com.

25.7. If the Pentest Audit shows any results that might impact Leaseweb, the Customer shall be obligated to share these results with Leaseweb at support@leaseweb.com.

25.8. For approval of other technical security activities not mentioned in this Clause 25, Customer shall submit a request via e-mail to Leaseweb at support@leaseweb.com.

CHAPTER F. DORA ADDENDUM TERMS

26. DORA ADDENDUM TERMS FOR FINANCIAL ENTITY AND CUSTOMER ICT TPP

26.1. These DORA Addendum Terms can be used by the Customer with no need for a separate DORA Addendum.

26.2. This Chapter F only applies if and insofar Customer (i) is a financial entity subject to DORA ("**Financial Entity**") , or (ii) Customer that provides ICT services as ICT third-party service provider to Financial Entities under DORA ("**Customer ICT TPP**") to the extent necessary to enable the Customer to comply with its obligations towards its customers and/or End Users that qualify as a Financial Entity.

26.3. Leaseweb is considered an ICT third-party service provider ("**ICT TPP**") under DORA. Leaseweb is not designated as a critical ICT third-party service provider under DORA. Leaseweb is not a financial entity. For the purpose of Customer questionnaires and information requested by Customer from Leaseweb for its obligation as Financial Entity under DORA or Customer ICT TPP, Customer can find more information on the Leaseweb Website under the header of Security & Certifications – DORA at https://www.leaseweb.com/en/about-us/security-certifications.

26.4. For the avoidance of doubt, Leaseweb itself is not subject to DORA and is not under the supervision of any European Supervisory Authority ("**ESA**"). Leaseweb's Legal Entity Identifier ("**LEI**") number is 72450035HURHH68XLR23. Thus, Customer cannot claim a LEI number from Leaseweb. In Leaseweb's role as ICT TPP Leaseweb and the Customer if qualified as Financial Entity hereby establish their mutual written contractual terms by means of this DORA Addendum under Chapter F of these Leaseweb Policies. Consequently, Leaseweb applies this DORA Addendum to the Sales Contract of the Customer, whereby the Customers has duly recognized and accepted its responsibility under DORA and related regulations.. For the purposes of Leaseweb's compliance with DORA, contractual transparency and efficiency Leaseweb shall not fill our and/or enter into any Customer specific questionnaires, agreements or DORA terms.

26.5. All Services and Support offered to the Financial Entity or Customer ICT TPP under DORA and these Policies are described and set forth in the applicable Sales Terms and Conditions, Services Specifications and Service Level Agreement ("SLA"). The location of the Services and the storage of such related data is in the Netherlands, unless the Customer has chosen a backup location outside of the Netherlands.

26.6. Leaseweb will provide assistance to the Customer in the form of Support in accordance with Chapter B of the SLA when an ICT-related Incident that is related to the provided Services occurs.

26.7. Leaseweb shall maintain appropriate business continuity measures to support continued provision of the Services, to the extent such obligations are related to the Services.

26.8. The Customer accepts in good faith that Leaseweb - by providing details of Leaseweb's security awareness training – has duly fulfilled its duty of participation in Financial Entity's ICT security awareness programs and digital operational resilience training. Leaseweb hereby demonstrates and reasonably assures the Customer that Leaseweb's own programs and trainings are appropriate for the purposes of DORA. Where additional training is specifically proven to be required under DORA, Financial Entity or Customer ICT TPP may reasonably request Leaseweb to participate in these security programs and training on the following conditions i) that Leaseweb receive a notice at least one (1) month in advance , and ii) that approval by Leaseweb is duly granted. Such participation will be in the form of a webinar and/or online meeting, or in-person training depending on availability of Leaseweb's designated reasonable scope of personnel to be confirmed by Leaseweb authorized senior management.

26.9. In fulfilling its role as ICT TPP under DORA, Leaseweb will cooperate with the competent authorities and resolution authorities of the Customer.

26.10. In the event of Leaseweb's insolvency, resolution in bankruptcy, or discontinuation of Leaseweb's business (other than as a result of an acquisition, merger or the like) that results or is reasonably likely to result in termination of the Service, or any termination of the Sales Contract with respect to a Service, unless prohibited by applicable law or regulations, Leaseweb will make Personal- and non-personal data within Leaseweb's control available in a reasonable manner under Leaseweb's standard processes under its Sales Contract Schedules upon written request by the Financial Entity.

26.11. For more information on Leaseweb's certifications and assurance reports, please visit: https://www.leaseweb.com/en/about-us/security-certifications.

27. CRITICAL OR IMPORTANT FUNCTIONS

27.1. In the event that Leaseweb in its role of ICT TPP supports the Customer with "critical or important functions" in accordance with Clause 30 (3) of DORA and the RTS, the following applies:

(i) Leaseweb shall facilitate reasonable procedures for coordinating access to its facilities and systems, provided that such procedures shall not limit or adversely affect the Customer, an appointed third party or Customer's competent authority's unrestricted rights of access, inspection and audit under DORA.

(ii) On-site or remote inspection rights:

a) Customer or its appointed third party shall have the right to on-site or remote inspections once every (1) year, by giving Leaseweb at least two (2) weeks advance notice.

b) Customer's Competent authority initiated emergency inspection: if a competent supervisory authority exercises its emergency powers under Clause 39 of the DORA, it may conduct on-site or remote inspection without prior notice.

(iii) Leaseweb will cooperate during such on-site inspection and audits performed by the competent authority, by Customer or its appointed third party.

(iv) Leaseweb shall reasonably apply the above to its selected subcontractors for Services that support the Customer for critical or important functions.

The conditions above are fully subject to prior additional contracts for confidentiality as well as safety and security measures, mutually agreed by Parties, including the selected Leaseweb subcontractor that support to critical or important functions, by means of a non-disclosure agreement or similar contract by and between the Customer also for and on behalf of its appointed third party entered in to with Leaseweb.

27.2. Leaseweb shall provide Customer with an adequate transition period allowing Financial Entity to migrate to another ICT third-party service provider in accordance with Clause 30 (3 f) of DORA.

27.3. Leaseweb shall notify Customer of ICT-related Incidents that adversely impact their use of the Services supporting critical or important functions in line with Service Levels via the existing notification channels. Upon Customer request, Leaseweb will provide based on its details and insights of the Incident a report with information on such ICT-related Incident. These notifications and additional reports are provided to Customer via these existing notification channels.

28. DORA TERMINATION RIGHTS

28.1. Without prejudice to the Financial Entity's rights to terminate the Sales Contract as set out in the Sales Terms and Conditions, the Financial Entity may terminate the Sales Contract by providing thirty (30) days' notice to Leaseweb ("**DORA Notice**"), such DORA Notice shall be substantiated by Financial Entity in detail including the ground for serving such notice, if:

(i) Leaseweb is in significant breach of applicable laws, regulations or contractual terms of the applicable Sales Contract in providing the relevant Services to Financial Entity;

(ii) If there are material changes affecting the Services in use by the Financial Entity or material changes that have an adverse impact on the provision of the relevant Services by Leaseweb;

(iii) Evidenced weaknesses pertaining to Leaseweb's ability to perform the Services are identified by Financial Entity or its appointed third party;

(iv) Where the competent authority can no longer effectively supervise Financial Entity as a result of the conditions of, or circumstances related to the Sales Contract; such termination is solely based on express instructions from Financial Entity's regulator.

28.2. Where Customer acts as ICT TPP towards its End User that qualifies as Financial Entity under DORA, the Customer ICT TPP may terminate the Sales Contract on the grounds set out in Clause 28.1 to the extent reasonably required for the Customer ICT TPP to comply with its obligations towards such Financial Entity under DORA.

28.3. Customer ICT TPP acknowledges and accepts that Leaseweb has no contractual relationship with Customer ICT TPP's End Users, including any regulated Financial Entity. Leaseweb disclaims any responsibility for Customer ICT TPP's regulatory and contractual compliance towards its End User. Leaseweb's contractual commitments solely apply to Customer ICT TPP excluding any liability towards Customer's ICT TPP's End User.

28.4. If the Sales Contract is terminated by making use of the DORA termination, the effects of termination & cancellation set forth in the Sales Terms and Conditions are applicable whereby the Customer shall be obliged to pay the Early Termination.

29. COSTS AND FEES

29.1. To receive Support from Leaseweb in connection with the exercise of the following rights, Customer agrees to pay to Leaseweb certain Fees and other related costs as determined by Leaseweb, such Fees will include and are not limited to:

(i) Support beyond the scope of the Services; Leaseweb may charge certain standard and special Fees for assistance in the form of Support with an ICT Event upon request by Customer for such Support as set forth in an Order, or Quotation.

(ii) Any cost related to access, recovery and return in an easily accessible format of Customer's data under Clause 26.6.

(iii) Any cost related to Leaseweb's participation in Customer's security awareness programs or digital operational resilience training under Clause 26.4 shall be borne by Financial Entity including venue, travel and other organizational expenses.

(iv) All such audit costs referred to in Clause 27 shall be borne by Customer.

CHAPTER G. FACILITY OPERATIONS POLICY

30. INTRODUCTION

30.1. The Facility Operations Policy contains a code of conduct for the day-to-day operations – and the presence of Customers – at a Data Center.

30.2. Leaseweb has adopted the Facility Operations Policy for the security and safety of Customers, Customer's employees, Customer's (sub)contractors and/or the Infrastructure.

31. SHIPMENTS

31.1. Each Customer shall observe the shipping and receiving policies adopted from time to time by Leaseweb with respect to shipment of its Equipment to and from the Data Center.

31.2. Customer shall notify Leaseweb of any intended shipment of its Equipment to the Data Center, at least two (2) business days before the intended delivery date of the Equipment. Such notification will be given by Customer by means of the shipment notification form available in the Customer Portal. In relation to administrative activities performed by or on behalf of Leaseweb in connection with such shipment, Leaseweb shall be entitled to payment by Customer of a shipment charge in the amount of: (i) fifty Euros (€ 50,--), in the event that Customer has timely notified Leaseweb of the intended shipment; or (ii) two hundred and fifty Euros (€ 250,--), in the event that Customer has not notified or has not timely notified Leaseweb of the (intended) shipment.

31.3. All costs related to Customer's shipments of Equipment to or from a Data Center shall be at Customer's cost and expense.

31.4. Customer is responsible for cleaning up and disposal of all materials and Equipment used for the shipping of Customer's Equipment. Customer shall ensure that such shipment material is removed from the Data Center on the same day as the date of delivery. If Customer does not comply with this provision, Leaseweb shall charge a cleanup fee to Customer.

31.5. Customer shall use its own company name and Business information as receiver/importer reference for any Customer or Customer third party supplier's initiated shipment, import and/or transport and customs documentation for any packages or letters to the Data Center for receipt by the Customer. All packages sent by Customer and/or by a Customer engaged third-party supplier to Customer at the Data Center shall be at Customer's own risk and expenses and Customer has the duty to fill properly fill out and submit all transportation and customers documentation accordingly. It is prohibited for the Customer to list or mention Leaseweb as receiving or importing party for such Customer or Customer third party supplier initiated Shipments. Leaseweb is not responsible for Customer's or Customer's Supplier initiated shipments to or from the Data Center. For the avoidance of doubt: Leaseweb cannot be used as importer of records by Customer of its Customer engaged third party supplier. Customer shall be solely and fully responsible for the compliance with any customs, export and import regulations.

31.6. The conditions of Packing Support in relation to transportation of Customer's Equipment from Leaseweb's Data Center are set out in Clause 15 of the Service Level Agreement.

32. PHYSICAL STORAGE

32.1. Data Centers have little or no storage area. Leaseweb cannot assure the safety of Colocated Equipment that is not secured in the Housing Space or contained within the Data Center.

32.2. If Customer is not yet ready to install the Equipment, Leaseweb may require Customer to store the Equipment in a designated storage area at Customer's expense. In case the Equipment remains in such storage area for more than fourteen (14) calendar days Customer shall pay Leaseweb Fees for the storage of the Equipment.

33. CONDUCT AT DATA CENTER

33.1. With the exception of an Emergency, Customer with a 24/7 access card shall give Leaseweb at least one (1) hour's notice for access to the Data Center and/or Housing Space, and Customer without a 24/7 access card shall give Leaseweb at least twenty four (24) hours' notice for access to the Data Center and/or Housing Space.

33.2. Customer shall identify itself at the reception of the Data Center by showing a valid ID (Driver's license, Passport, Country ID) and explain the purpose of its visit. Customer is required to sign in and out when entering and exiting the Data Center, whereby Customer shall indicate its time of entry and time of exit. The reception will hand over an access card. Customer shall at all times during the visit wear the access card which needs to be fully visible. Before leaving, Customer shall - at the reception – hand in the access card; failure to do so may result in additional Service Fees.

33.3. On a daily basis, Customer may allow a maximum of three (3) persons to access the Data Center. A Service Fee shall be due by Customer for each person entering the Data Center, with the exception of a holder of a 24/7 access card or those persons who are accompanying such card holder access card. Only the first person will be charged. Access shall be charged on a thirty (30) minutes interval basis, with a minimum of one (1) hour.

33.4. Customer shall provide Leaseweb with a list of persons authorized for access to the Housing Space and Colocated Equipment, which Customer may amend from time to time upon written notice to Leaseweb. Customer shall be responsible for all persons who receive access on behalf of Customer.

33.5. Leaseweb may require, at its sole discretion, that a Leaseweb representative escorts any representative of Customer accessing the Data Center and/or Housing Space. Also, the house rules of the Data Center may provide that the owner or lessor of the Data Center may - under certain circumstances - require that one of its staff escorts any representative of Customer who are accessing the Data Center and/or Housing Space.

33.6. If Leaseweb personnel provides an escort during Customer's access to the Data Center and/or Housing Space, such escort shall be considered an additional Service for which Leaseweb shall charge Customer an additional Service Fee (escort Fee) in addition to all escort Fees imposed on Leaseweb by the Data Center owner. If a representative of Customer is accompanied by an escort provided by the owner or lessor of the Data Center while accessing the Housing Space, Customer shall pay Leaseweb all related escort Fees that may be imposed on Leaseweb.

33.7. Customer shall (i) at all times, act in a professional manner, (ii) not interfere in any way with Leaseweb's use or operation of the Data Center or with the use or operation of any Equipment installed by other parties, including Equipment of other Customers. Should Customer require to (re)move or disconnect another party's Equipment to service its own Equipment, Customer shall contact Leaseweb and request Leaseweb's instructions prior to any such movement, removal and/or disconnection, taking into account a 48 hour notice period, (iii) refrain from operating any Equipment that may constitute a safety hazard, (iv) not perform any tests that may cause harm or damage to – or interfere with – the Leaseweb Network, the Housing Space and/or the Data Center, and (v) ensure that it closes doors after use, in order to maintain a closed and secure environment and thus ensuring an efficient environment for the fire protection system and climate control system, and (vi) lock the Rack before leaving. If in doubt, Customer shall consult the facility manager of the Data Center or – in the facility manager's absence – another employee of Leaseweb.

33.8. Leaseweb may at its sole discretion remove any of Customer's personnel or Customer's (sub)contractors or third party agents, if such person does not comply with any Leaseweb Policy, or any instruction provided by an employee of Leaseweb.

33.9. In case of an Emergency, such as a fire, which in general will be indicated by the sound (slow whoop) of an alarm system, Customer shall immediately evacuate the Data Center.

33.10. Smoking is prohibited in the entire Data Center. Eating and drinking is prohibited in the areas within the Data Center where the Housing Space and/or Equipment is located.

33.11. Within the areas where the Housing Space and/or Equipment is located, Customer shall refrain from any activity that may cause dust particles. One of the reasons for this prohibition, is that dust particles may set off the automatic alarm system. If in doubt, Customer shall consult the facility manager of the Data Center or – in the facility manager's absence – another employee of Leaseweb.

33.12. Unless expressly required under any (product)insurance warranty, Customer shall not bring any packaging material into the areas where the Housing Space and/or Equipment is located and any (cardboard) boxes shall be unwrapped by Customer in the loading bay area. Should Customer - in view of a (product)insurance warranty - require to bring packaging material into the areas where the Housing Space and/or Equipment is located, it will notify Leaseweb thereof in advance. Leaseweb will then assign a member of its staff to accompany Customer during Customer's presence in the areas where the Housing Space and/or Equipment is located. Customer is under an obligation to remove all packaging material from the areas where the Housing Space and/or Equipment is located, within one (1) hour after entering the relevant area.

33.13. Customer shall immediately report any irregularities and/or alarms, noticed by Customer during its presence in the Data Center, to the facility manager of the Data Center or – in the facility manager's absence – another employee of Leaseweb.

34. EQUIPMENT REQUIREMENTS

34.1. Unless expressly agreed otherwise in writing by Leaseweb, all Equipment shall be installed and maintained by or on behalf of Customer in accordance with the following criteria: (i) Telecommunication lines shall be extended from an organized and protected distribution frame; (ii) Spare parts for the Equipment shall be kept within the confines of the Housing Space; (iii) AC and DC power distribution shall take place within the Housing Space, to the extent available; (iv) Equipment density shall be consistent with floor loading at the Facility; (v) All cables shall be tied and harnessed in an orderly fashion; (vi) Equipment shall be in full compliance with telecommunications industry standards and in accordance with Leaseweb's requirements and specifications; (vii) all Colocated Equipment and associated cabling shall be installed in such a way that the related cabinet can be closed and locked; and (viii) Equipment shall comply with applicable laws, rules and regulations in the jurisdiction where located and in addition as applicable in the EU (including specifically, but without limitation, the EU EMC Directive (89/336/EEC) and the EU Low Voltage Directive (73/23/EEC)), as amended from time to time.

34.2. Customer is expressly prohibited from installing any AC UPS Equipment in the Housing Space or at the Data Center in general.

34.3. Customer must ensure that Equipment with AC power supplies have a power factor of 0.85 or higher.
Leaseweb utilizes a hot aisle-cold aisle configuration, meaning each Rack has a designated cold side and hot side to ensure optimal cooling efficiency. Customer shall install all of its Equipment in alignment with this airflow, with the air inlet on the cold side and the outlet on the hot side of the Rack ("**Conditioned Airflow**"). Incorrect Conditioned Airflow direction is strictly prohibited. Customer shall ensure that any of its unused Rack(s) are covered with blanking panels to ensure optimal cooling within the Data Center Hall. Leaseweb shall notify Customer upon identification of any violation of the Conditioned Airflow by Customer. Customer is responsible for ensuring all of its Equipment are compatible with the Conditioned Airflow as described in this Clause. Customer shall not deploy any Equipment which cause inverted airflow issues. In case Customer fails to comply with the Conditioned Airflow requirements as set out in this Clause Leaseweb shall not be held liable for any cooling problems or Equipment malfunctions and Customer shall not be entitled to receive Service Credits from Leaseweb.

CHAPTER H. INVESTIGATION AND ENFORCEMENT POLICY

35. INVESTIGATION

35.1. Leaseweb reserves the right to conduct an investigation, based on (i) suspected violations of the Policies; and/or (ii) (potential) security risks to its Infrastructure; and/or (iii) a valid request of the relevant (law enforcement) authorities (including a Digital Services Coordinator), and reserves the right to take action based on the outcome of such investigation.

35.2. As part of this investigation, Leaseweb may, acting reasonably (i) gather information from or about Customer; (ii) if relevant, gather information from a complaining party; and/or (iii) review and investigate Customer's security log(s) Customer is obliged to fully cooperate with any such investigations by Leaseweb.

36. LEASEWEB'S ACTION(S)

36.1. To the extent legally required, Leaseweb is authorized to grant relevant law enforcement authorities (including a Digital Services Coordinator) access to Customer's content, information and/or Infrastructure, as well as any information gathered in the investigation conducted by Leaseweb this Chapter.

36.2. Upon request of a third party, a law enforcement authority (including a Digital Services Coordinator), Leaseweb shall be entitled to disclose identifying Customer information to said party in connection with a (suspected) breach of the Leaseweb Policies to the extent required by law

(such to be determined in Leaseweb's discretion). Leaseweb has adopted technical and organizational measures to prevent unlawful governmental access or transfer of Customer data held in the EU.

36.3. Leaseweb shall be entitled to take action, legal or otherwise, against Customer and/or and End User, in the event that the use of the Service by Customer or its End User(s), breaches the Policies, or Customer allegedly fails to comply with any obligation under the Policies. The appropriate action will be determined by Leaseweb, in its sole discretion, and may include: (a) suspension or termination of any or all of the Services in accordance with the Sales Terms and Conditions; (b) (selective) IP or port blocking; (c) reinstallation of the Services; (d) imposing limits on the use of Service (such as imposing limits on the speed of the data the Customer may transmit and/or receive with the Service); (e) restarting the Service, (f) blocking access at the router and/or switch level of Customer's Infrastructure; (g) denying Customer (physical) access to Infrastructure; (h) providing binding instructions to Customer in regards of the use of the Services, (i) changing or updating Customer PTR, rDNS or rWHOIS records; and/or (j) placing files infected by Malicious Software in quarantine.

36.4. To enhance transparency and compliance with the DSA, Leaseweb may publish reports outlining its content moderation practices, including the number and nature of content removals and Customer accounts suspended or terminated.

36.5. Leaseweb herewith informs Customer that if Leaseweb becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.

37. DISCLAIMER

37.1. Without prejudice to the above or any other provision of the Policies, Leaseweb does not (and does not intend to) review, monitor or control as a precautionary measure content stored, sent or received by Customers using the Services. Leaseweb is not responsible or liable for the content of any communications that are transmitted by or made available to Customer or its End Users, regardless of whether they originated from the Network or the Services.

37.2. None of the provisions of this Chapter H or any of the other Chapters of the Policies shall in any way limit or prejudice any other rights or remedies Leaseweb may have.

CHAPTER I. DATA ACT

38. SWITCHING PROCESS

38.1. Leaseweb shall cooperate with the Customer in good faith to make the switching process effective.

38.2. Leaseweb as service provider of the unmanaged IAAS delivery model without having access to the Customer's operating services, software and applications stored on Leaseweb's infrastructure as referred to in Articles 26 and 30 sub 1 of the Data Act, requires the Customer itself to enable its timely transfer of its Customer Data (during the Transition Period and in any case not later than the end of the Data Retrieval Period). Thereby Leaseweb shall maintain the continuity of the Services under the ongoing Sales Contract while the Customer is enabling such transfer of its Customer exportable data and digital assets.

38.3. As per Leaseweb's IAAS delivery model of Services, Leaseweb facilitates functional equivalence to take reasonable measures in its switching process for new Customers and Customers that submitted a Switching Request both aimed a minimum level of functionality of services before and after the switching process. In case Customer requests from Leaseweb Services of which the majority of main features need to be custom-built to respond to Customer's specific demands or where all components have been developed for Customer's purposes, Leaseweb's obligations on functional equivalence set forth in this Clause shall not apply.

38.4. Customers retain the right to access and retrieve the data generated through their use of the Service or any related Service in machine-readable formats.

38.5. For information purposes on the switching process, Leaseweb provides more information on technical aspects, capabilities, technical support and necessary tools to the extent feasible and applicable for the switching process in the Knowledge Base available on www.leaseweb.com (Leaseweb's Knowledge base as referred in Clause 42 of the Service Specifications).

38.6. For Leaseweb's adherence to the Data Act transparency obligations for the respective jurisdictions where the Leaseweb infrastructure is located in the European Union, Leaseweb makes refence to its Website (www.leaseweb.com/en/about-us/legal/sales-contract) where the printable, downloadable versions of the Sales Contacts in full transparency are made available to the Customer prior to ordering the Services. This Website is listed in the Sales Contract.

38.7. In addition to this Clause of the Policies for the switching process under the Data Act, the applicable rights and obligations of Leaseweb and the Customer are further described in Clauses 10.5, 21.6-21.11 and 22.10 of the Sales Terms and Conditions.

39. DATA ACT TERMS

39.1. With respect to the transparency obligations set out in the Data Act Leaseweb refers to Clauses 8 and 28 of the Sales Terms and Conditions covering (i) the jurisdiction where Services are deployed; and (ii) information on the technical and organizational measures adopted by Leaseweb in relation to international governmental access or transfer of non-personal data (Article 28 of the Data Act on contractual transparency obligations on international access and transfer). For further information please visit https://www.leaseweb.com/en/about-us/legal/sales-contract; https://www.leaseweb.com/en/about-us/legal/personal-data-protection-acts; https://www.leaseweb.com/security-certifications.

39.2. As a rule Services are not considered to qualify as "connected product" and "related service" under the Data Act. However, to the extent that Services can be considered as "related service", as defined in the Data Act, information on such "related service" is deemed provided through the Customer's use of and access to the Services.

CHAPTER J. DATA LOCALIZATION AND DATA SOVEREIGNTY

40. DATA LOCALIZATION

40.1. Leaseweb's infrastructure is physically located in the Netherlands, at the following locations, and is subject to the local jurisdiction and applicable laws of the Netherlands:
   a) J.W. Lucasweg 35, 2031 BE Haarlem, The Netherlands (AMS-01 Data Center);
   b) Capronilaan 2, 1119 NR Schiphol-Rijk, The Netherlands (AMS-02 Data Center).

40.2. For Colocation Services, where multiple local Data Center locations are available, the Data Center location of Customer's Colocation Equipment is determined by the Customer.

41. DATA SOVEREIGNTY

41.1. For the purpose of maintaining data sovereignty, where Customer data is processed and stored by Leaseweb, such processing and storage occurs only in Data Center(s) located strictly within the Netherlands, subject to the laws of the Netherlands.

CHAPTER K. TECHNICAL AND ORGANIZATIONAL MEASURES ("TOMS")

42. TECHNICAL AND ORGANIZATIONAL MEASURES - GENERAL

42.1. Leaseweb has implemented the technical and organizational security measures following among other the specific requirements under the GDPR. In view of the GDPR, Leaseweb has taken and will maintain the appropriate technical and organizational security measures for protection of the security, confidentiality and integrity of (customer's) Personal Data as described below.

42.2. Leaseweb not only assures a level of security but also of cybersecurity and business resilience which follow from Leaseweb obtaining the following certifications and assurance reports: ISO 27001, ISO 14001, NEN7510, SOC1, PCI DSS.

42.3. The relevant security certifications of Leaseweb's Data Center providers are listed on the Website available via the following link: https://www.leaseweb.com/en/why-leaseweb/platform/data-centers.

43. TECHNICAL MEASURES

43.1. Leaseweb has implemented the following technical measures:
   a) **Data Encryption:**
      - Full disk encryption of all Leaseweb managed employee endpoints (data at rest).
      - Leaseweb has strong cryptography & security protocols with respect to data transmission via TLS or VPN (data in transit).
   b) **Access Controls:**
      - Access permissions based on least-privilege and need-to-know.
      - Leaseweb has policies and procedures in place for on- and offboarding of Leaseweb employees with regards to access management.
      - Robust authentication and password related policies are in place and monitored.
      - Tools are made available to enable Leaseweb employees to work securely (such as password manager, VPN client, endpoint protection on all Leaseweb employee endpoints).
   c) **Secure Development:**
      - Code changes require a six-eyes principal.
      - (Security) Configuration of servers is based on infrastructure-as-code where possible.
      - All development teams are audited by the Leaseweb's security team twice a year based on a security maturity model.
      - Segregation between development, test and production environments.
      - Version control on Leaseweb's codebase.
   d) **Network Security:**
      - Network segmentation on Leaseweb's internal networks.
      - Firewalls are used in Leaseweb's internal network.
      - Intrusion detection systems are used within Leaseweb's internal network.
   e) **Vulnerability Management:**
      - Anti-virus software with EDR capabilities is installed on every Leaseweb employee endpoint to detect and stop the abuse of vulnerabilities.
      - Vulnerability monitoring, pentesting and red-teaming exercises are performed.

43.2. Leaseweb may update these measures from time to time to adapt to evolving threats and technologies.

44. ORGANIZATIONAL MEASURES

44.1. Leaseweb has implemented the following organizational measures:
   a) **Information Security Governance:**
      - Leaseweb operates an Information Security Management System ("ISMS"), conforming to the ISO 27001standard.
      - This ISMS is audited on an annual basis by internal as well as external auditors.

- Periodic contact with interested parties, such as security service providers, government and peer organisations to exchange threat intelligence and vulnerability information.
- Leaseweb has a dedicated IT Security department.

b) **Data Deletion:**
- Wiping of Leaseweb equipment in use by Customer after termination of the Sales Contract.
- Physical destruction of broken hard drives.
- Secure paper disposal facilities are available.

c) **Employee Training:**
- Leaseweb employees have periodic mandatory security awareness training with varying topics including privacy awareness.
- Periodic phishing simulations for all Leaseweb employees.

d) **Risk management:**
- Security risk assessments are performed on a periodic basis.
- A security risk register is maintained and updated.

e) **Vendor Management:**
- Data centers and offices are secured to prevent unauthorized access.
- Periodic vendor screening to evaluate and manage risks related to existing and new vendors.

f) **Physical Security:**
- Data centers and offices are secured to prevent unauthorized access.:
- Periodic reviews of physical security authorizations.

g) **Documentation and Record-Keeping:**
- Leaseweb maintains records of security policies and procedures.
- Records are kept in our internal documentation and are updated periodically.

h) **Continuous Monitoring of Leaseweb's internal IT environment by:**
- Security information and event management ("SIEM") tooling
- A third-party Security Operating Center ("SOC") that monitors the internal IT environment.

i) **Audits and certifications:**
- Internal auditing: Leaseweb performs internal audits on security related controls on a yearly basis.
- External auditing:
  - PCI-DSS 4.0 certified,
  - ISAE3402 type 2 (SOC1) assurance report,
  - ISO 27001:2022 certified,
  - ISO 14001, and
  - NEN 7510:2017 assurance report.

44.2. Leaseweb may update these measures from time to time to adapt to evolving threats and technologies.

CHAPTER L. LEASEWEB'S SUB-PROCESSORS LIST

45. SUB-PROCESSORS ENGAGED BY LEASEWEB

45.1. Leaseweb may engage Sub-Processors for the delivery of the Services, including affiliates and third parties. The type of Services provided to Customer determines the relevant Sub-Processors used for the performance of the Services.

45.2. Leaseweb engages the following Sub-Processors for all Services:

Affiliate Sub-Processor	Purpose	Location
Leaseweb Global B.V. Address: Hessenbergweg 95, 1101CX Amsterdam	IaaS Service.	The Netherlands
Leaseweb Network B.V. Address: Hessenbergweg 95, 1101CX Amsterdam	This Affiliate entity of Leaseweb provides on request of Leaseweb certain network services.	The Netherlands