Version: 2021.1

Addendum to the Sales Contract
DATA PROCESSING AGREEMENT LEASEWEB AS PROCESSOR

PARTIES:

1. [……], a private company with limited liability, having its registered seat at [……] and its office at [……] at the [……] ("**Customer**");

and

2. **LEASEWEB USA, INC.**, a Delaware Corporation, with its registered office at 9301 Innovation Drive/Suite 100, Manassas, VA 20110, the United States of America ("**Leaseweb**");

Customer and Leaseweb will also individually be referred to as a "**Party**" and together as the "**Parties**".

INTRODUCTION:

A. Leaseweb is part of one of the world's largest hosting brands, providing Infrastructure-as-a-Service (IaaS) hosting solutions to its customers worldwide, ranging from SMBs to enterprises (the "**Services**"). The Services include Public Cloud, Private Cloud, Dedicated Servers, Data Storage, Cybersecurity, Colocation, Managed Hosting, and Hybrid Solutions.
B. The Parties entered into the Sales Contract (as defined in Section 1.2 below) pursuant to which Leaseweb shall provide to Customer those certain Services specified on the Order Form(s) or the Order Confirmations executed by the Parties thereunder.
C. In the performance of Leaseweb's obligations under the Sales Contract in particular for the purpose of storage on behalf of Customer, Leaseweb and its Affiliates shall Process Personal Data for or on behalf of Customer. The Parties acknowledge and agree that with regard to the Processing of Personal Data on Customer's behalf, Customer is the controller, and Leaseweb is the processor. Furthermore, the Parties are aware that Leaseweb's role as processor in its capacity as an IaaS provider is limited.
D. In order to comply with applicable laws with respect to the Processing of Personal Data by Leaseweb, the Parties agree upon the conditions as set forth in this Data Processing Agreement ("**DPA**").

HAVE AGREED AS FOLLOWS:

1. APPLICATION, SCOPE, AND DEFINITIONS

1.1 **Application.** This DPA forms part of, applies to, and (to the extent of any conflict) takes precedence over the Sales Contract. In the event of a conflict between this DPA and an Order, the Order shall prevail.

1.2 **Scope.** This DPA applies to all Customer Data and all access to Customer Networks in connection with the Sales Contract. Appendix 1 of Annex 2 of this DPA provides background on the subject matter, nature, purpose and duration of the Processing, and additional detail.

1.3 **Definitions.** For purposes of this DPA:

1.3.1 "**Affiliate**" means in relation to a party, any entity which (directly or indirectly) controls, is controlled by and/or under common control with that party.

1.3.2 "**The Sales Contract**" means the Contract pursuant to which Leaseweb provides certain Services to Customer, together with any related contractual document between the Parties, including (without limitation) the Sales Terms and Conditions, the Support and Service Levels, the Leaseweb Policies, and the Services Specifications thereunder.

1.3.3 "**Applicable Law**" means all applicable laws, regulations, legally binding directions from a regulator, and other applicable legal requirements of any jurisdiction, such as, to the extent applicable, the GDPR.

1.3.4 "**Authority**" means the authority that is engaged to supervise the processing of Personal Data within the meaning of Article 4 paragraph 21 and Article 51 GDPR - and Data Subject(s).

1.3.5 "**Customer Data**" means Personal Data that Leaseweb receives from Customer, or otherwise Processes for or on behalf of Customer, in connection with the Sales Contract.

1.3.6 "**Customer Networks**" means any hardware, software, networks or other information technology resources owned or operated by Customer, other than any that are owned by Leaseweb (or by its Subprocessors in their role as Subprocessors).

1.3.7 "**Data Breach**" means a confirmed instance of accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Customer Data, or other accidental, unlawful or otherwise unauthorized Processing of Customer Data.

1.3.8 **"Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

1.3.9 "**GDPR**" means the General Data Protection Regulation (Regulation (EU) 2016/679).

1.3.10 "**Personal Data**" means any information relating to an identified or identifiable individual, within the meaning of the GDPR (regardless of whether the GDPR applies).

1.3.11 "**Process**" and "**Processing**" mean any operation or set of operations performed on Customer Data or on sets of Customer Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination

or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.3.12 "**Standard Contractual Clauses**" means the document set forth in Annex 2 attached hereto.

1.3.13 Any defined terms used but not defined herein shall have the meaning set forth in the Sales Contract.

2. PROCESSING

2.1 Leaseweb shall Process Customer Data only if and to the extent such Processing is required and permitted in the performance of the Sales Contract by Leaseweb (such as the performance of support), and on other legal grounds such as legitimate interests. If Leaseweb is under a legal obligation to Process the Customer Data, Leaseweb shall inform Customer of such legal obligation unless it is prohibited by law or reasons of important public interest from doing so.

2.2 Leaseweb will endeavor to arrange that only authorized personnel shall have access to the Customer Data.

2.3 Leaseweb shall not retain the Customer Data of Customer longer than is necessary for (i) the performance of the Services; or (ii) complying with any statutory obligation of Leaseweb.

2.4 Customer acknowledges that Leaseweb does not control and does not act as controller of any Customer Data or other content transmitted over the Customer Networks.

3. SUBPROCESSORS

3.1 Leaseweb is entitled to sub-contract any of its obligations under this DPA to any of its Affiliates or to any third-party (each a "**Subprocessor**"), without the prior written approval of Customer. Upon request, a list of any such third party Subprocessor shall be provided to Customer.

3.2 In the event Leaseweb engages Subprocessors in the performance of this DPA, Leaseweb shall impose on each such Subprocessor's data protection obligations that are the same as or substantially similar to Leaseweb's own obligations under this DPA.

4. SECURITY

4.1 When Processing Customer's Personal Data under this DPA, Leaseweb shall employ adequate technical and organizational precautions and measures. Whether the measures are sufficient and suitable, will be determined based on the state of the art, costs of implementation, the nature, scope, context and purposes of the Processing as well as the risk of such Processing. Leaseweb shall take, and shall ensure that any Subprocessors take adequate necessary technical and organizational precautions and measures.

4.2 The security measures referred to in Clause 4.1 must satisfy the applicable requirements imposed by the Data Protection Laws, and in any case will include the following certifications: ISO 27001, NEN7510, SOC1, PCI DSS, CISPE. Upon reasonable request by Customer, Leaseweb shall provide an overview of the security measures that is has in place; provided, however,

that such overview shall be general in nature in order to safeguard the integrity of such security.

5. NOTIFICATION DUTY

5.1 In case of a Data Breach Leaseweb shall notify Customer without undue delay after discovery of such Data Breach. Such notification shall be in accordance with Clause 5.2.

5.2 The Parties agree that Leaseweb, in case of a Data Breach, shall - without undue delay - inform Customer in writing (e-mail is allowed) to Customer. Leaseweb shall inform the following contact persons of Customer: [name], [title], [telephone], [email].
If any alterations are made by Customer with regards the above contact details, Customer will inform Leaseweb directly. If Customer fails to do so, the (possibly negative) consequences thereof are borne by Customer.

5.3 Leaseweb shall provide Customer in its notification with all necessary information, including but not limited to (i) the nature of the Data Breach, including the categories and approximate number of Data Subjects and records concerned; (ii) the contact at Leaseweb who will liaise with Customer with respect to the Data Breach; (iii) the probable consequences of the Data Breach on the (Processing of) the Personal Data; and (iv) the remediation measures taken by Leaseweb to mitigate and contain the Data Breach.

5.4 In those instances in which a Data Breach would not have occurred if Leaseweb had not obviously at its own discretion taken or failed to take some specific material act with substantial impact, Leaseweb will, if requested in writing by Customer, (i) notify the Data Subjects and the Authority of the Data Breach in a form reasonably acceptable to Customer (and refrain from making such notification without Customer's written consent unless required by Applicable Law), and/or (ii) provide reasonable assistance to Customer in notifying the Authority regarding the Data Breach.

6. TRANSFER OF PERSONAL DATA

6.1 Leaseweb shall only Process Personal Data in countries outside the European Economic Area that ensure an adequate level of protection, in line with the applicable Data Protection Laws and with prior written approval of Customer. If Customer requests Leaseweb to Process Personal Data outside the European Economic Area, Customer represents that it has the legal authority and consents necessary to transfer the Personal Data in that manner.

6.2 The Standard Contractual Clauses attached hereto as Annex 2 apply and take precedence over the rest of this DPA to the extent of any conflict.

6.3 The supplemental clauses set forth in and attached hereto as Annex 3 ("**Supplemental Clauses**") apply.

7. AUDIT

7.1 Leaseweb is frequently being audited by external parties to ensure it complies with relevant normative frameworks and controls within the Leaseweb Circle of Trust model. See https://www.leasewebLeaseweb.com/certifications for more information.

7.2 Customer has the right, upon its request and under the conditions as specified in this Clause 7, to have an independent auditor conduct an audit regarding the organization of Leaseweb, in order to establish whether or not Leaseweb complies with the applicable Data Protection Laws and the DPA.

7.3 Such an audit shall take place only after Customer has requested Leaseweb to present it with an internal audit report; and if, after having reviewed such an internal audit report, Customer can substantiate why an additional external audit is justified. Such an external audit is justified if the internal audit report does not establish, or insufficiently establishes, whether or not Leaseweb complies with the applicable Data Protection Laws and the DPA. Customer may request an external audit once every two (2) years, giving Leaseweb two (2) weeks' notice in advance, notwithstanding the compelling reason as referred to in Clause 7.4.

7.4 Leaseweb will cooperate with the external audit upon request of Customer and provide Customer with all information that can reasonably be deemed relevant, within a reasonable period of time. The Parties agree that a period of two (2) weeks is reasonable, unless a compelling reason requires more immediate action.

7.5 Prior to the external audit upon request of Customer, the Parties shall establish in writing whether the results of such an audit shall be subject to review and discussion of the Parties, or that the results will be accepted irrevocably. If it is established that Leaseweb has failed to comply with the provisions of applicable Data Protection Laws and the DPA, Leaseweb shall take all reasonably necessary measures to ensure compliance going forward.

7.6 The costs of audits upon request of Customer, will be borne by Customer, unless the results of such an audit show that Leaseweb has failed to comply with the provisions of applicable Data Protection Laws and the DPA.

8. DATA SUBJECTS

8.1 In case a Data Subject wishes to exercise its rights under the Data Protection Laws, Leaseweb shall cooperate to the extent that can reasonably be expected of Leaseweb to ensure Customer can comply with its statutory obligations in this respect.

8.2 If and when a Data Subject, in the course of exercising its rights under the Data Protection Laws, reaches out directly to Leaseweb, Leaseweb shall forward such contact to Customer without undue delay and shall abstain from giving any substantive reply thereto, other than indicating the matter is being handled by Customer.

9. INDEMNIFICATION

9.1 Customer indemnifies Leaseweb from and against all claims by third parties, including data subjects, asserted against Leaseweb due to a breach of the Data Protection Laws or other applicable regulations concerning the processing of Customer Personal Data, or the DPA, that is attributable to Customer or third parties engaged by Customer. If such breach causes a measure or fine to be imposed on Leaseweb by the Authority, Customer shall also indemnify Leaseweb for all costs resulting therefrom.

9.2 Customer shall take out insurance sufficient to cover any payment that may be required under this Clause 9 and provide Leaseweb with the policy on request.

10. LIMITATION OF LIABLITY

10.1 Any liability of Leaseweb under this DPA is limited to the affected Services and to the amount (excluding VAT) invoiced by Leaseweb under the Sales Contract and timely paid by Customer, in the three (3) months prior to the day on which the liability arises, with a maximum of twenty-five thousand euros (EUR 25.000) per damaging event or series of damaging events.

10.2 In no event shall Leaseweb be liable under or in connection with this DPA for any indirect, Data Breach or consequential damages (including but not limited to: lost opportunities, loss of turnover, profits or goodwill, loss, mutilation or destruction of data or data files, and damages for liability towards third parties).

10.3 All of Customer's claims on Leaseweb, on whatever grounds, including but not limited to breach of DPA or tort, shall expire and cease to exist after a period of twelve (12) months following the day of the damaging event, if Customer fails to inform Leaseweb of the existence of such claim(s) and has failed to bring the claim(s) before the authorized court within the aforementioned period of twelve (12) months.

11. TERM AND TERMINATION

11.1 The DPA shall become effective upon signing by both Parties.

11.2 The term of the DPA is equal to the term of the Sales Contract. The Parties agree upon a 'phase out-period' of one (1) month, during which the obligations of the DPA shall still be applicable after the Sales Contract has ended. The DPA cannot be terminated prior to the expiration or termination of the Sales Contract.

11.3 Upon termination or expiration of the Sales Contract for whatever reason, Leaseweb shall delete all the Personal Data pertaining to Customer, including copies thereof, unless Leaseweb is required to retain such Personal Data under applicable law. If required by law to retain a copy, to the extent not prohibited by law or order of a court or regulatory authority, Leaseweb shall inform Customer what it is retaining and the legal reason why it needs to be retained.

11.4 The Clauses of the DPA that are intended to remain in force after the DPA has terminated or expired for whatever reason, shall remain in force after termination or expiration of the DPA, including but not limited to Clause 13 and this Clause 11.4.

12. MISCELLANEOUS

12.1 No change or amendment to or modification of the DPA shall be valid unless in writing and signed by both Parties.

12.2 Should any provision of the DPA be declared invalid for any reason, such decision will not affect the validity of any remaining provisions which will remain in force and effect. In any such event, the Parties will endeavor to replace the invalid provision with a provision of equivalent effect.

13. APPLICABLE LAW AND COMPETENT COURT

13.1 This DPA and all matters regarding the construction, interpretation or enforcement thereof shall be governed by the laws of the Commonwealth of Virginia.

13.2 Any matters or disputes arising in connection with the DPA, its subject matter or the legal relationship between Leaseweb and Customer shall be exclusively heard by the or federal courts of Prince William County, Virginia, USA.

For and on behalf of	For and on behalf of
Leaseweb USA, Inc.	[……]
_____	_____
Name:	Name:
Position:	Position:
Date:	Date:

ANNEX 1 –TECHNICAL AND ORGANIZATIONAL MEASURES

Leaseweb has implemented the following security measures in its organization:

- Network segmentation
- Next generation firewalls
- Anti-virus software
- Full disk encryption of end-points
- Encrypted communication via SSL or VPN
- Security Information and Event Management solutions
- Dedicated Security Operating Centre
- Security Awareness training
- Segregation of duties
- Role-based access permissions (based on least-privilege)
- Secure disposal facilities of confidential information
- Periodic pen testing of public facing services
- Secure development training
- Integrated security monitoring during development
- Tools to enable employees to work secure (such as password managers)
- Physical security zones

Per application or communication, additional security measures can be implemented.

Leaseweb is frequently being audited by external parties to ensure it complies with relevant normative frameworks and controls within the Leaseweb Circle of Trust model. See https://www.leaseweb.com/certifications for more information.

ANNEX 2 –Standard Contractual Clauses

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:.....

Address: .....

Tel.:.....; fax: .....; e-mail:.....

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: **Leaseweb USA, Inc.**

Address: 9301 Innovation Drive / Suite 100, Manassas, VA 20110, USA

Tel.: +1 571 814 3777; fax: +1 571 814 3777; e-mail: support@us.leaseweb.com

Other information needed to identify the organisation:

……
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or

unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the

subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Leaseweb USA Inc.

Position: CEO, President, Alexander Boost

Address: 9301 Innovation Drive / Suite 100, Manassas, VA 20110, USA

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer): The data exporter is Customer, a user of the Services, and all Affiliates of Customer established within the European Economic Area (EEA) and the United Kingdom that have purchased Services pursuant to the Sales Contract.

Data importer
The data importer is (please specify briefly activities relevant to the transfer): Leaseweb USA, Inc., for itself and on behalf of its Affiliates and customers.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify): Data exporter's employees, suppliers, prospects, customers or end users, or other third parties as determined by data exporter.

Categories of data
The personal data transferred concern the following categories of data (please specify): Business contact name, business address, e-mail address, work phone number, and bank details relating to data exporter's customer account with Leaseweb USA, Inc.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify): Data exporter may, in its sole discretion and to the extent determined by it, submit to the Services information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify): Processing for the provision of Services as set forth in the underlying Sales Contract.

Anticipated Duration of Processing
For the term of the Sales Contract, except where a different time is set forth in the Sales Contract.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name: Leaseweb USA, Inc.

Authorised Signature: Alexander Boost, CEO and President.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Leaseweb will comply with Annex 1 to the DPA.

ANNEX 3 –SUPPLEMENTAL CLAUSES

The Supplemental Clauses set forth in this Annex 3 form part of the that certain Data Processing Agreement ("**DPA**") by and between Leaseweb USA, Inc. ("**Leaseweb**") and ("**Customer**"). All defined terms used but not defined herein shall have the meaning set forth in the DPA.

1. To prevent the acquisition of the Customer Data by third parties, such as governmental authorities who may gain physical access to the transmission mechanisms (e.g., wires and cables) while the data is in transmission or at rest, the Parties shall encrypt the following: (i) transfers of the Customer Data between the Parties and by Leaseweb internally or to third parties, and (ii) the Customer Data when it is in storage or otherwise not in transit. To the extent permitted by Applicable Law or order, Leaseweb will only access Customer Data transmitted in plain text in the normal course of business pursuant to the Sales Contract (including in support cases) with the express or implied consent of Customer and/or the Data Subject to which such Customer Data pertains.
2. Leaseweb represents and warrants that it is not the type of provider that is eligible to be subject to Upstream collection ("bulk" collection) pursuant to Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a ("**FISA Section 702**"), as described in paragraphs 62 & 179 of the judgment in the EU Court of Justice Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, and that therefore the only FISA Section 702 process it could be eligible to receive would be based on a specific "targeted selector" (i.e., an identifier that is unique to the targeted endpoint of communications subject to the surveillance).
3. If Leaseweb receives a FISA Section 702 order seeking disclosure of the Customer Data, Leaseweb will (i) use all available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto, (ii) seek available interim measures to suspend the effects of the order until the court has decided the foregoing challenges on the merits, (iii) not disclose the Customer Data requested until required to do so under the applicable procedural rules, (iv) provide the minimum amount of information permissible when responding to the order, based on a reasonable interpretation of the order, and (v) notify the requesting governmental authority that because the CJEU has deemed FISA Section 702 orders incompatible with the safeguards contained in the GDPR's Article 46 transfer tool, the order gives rise to a potential conflict of laws. To the extent not prohibited by Applicable Law or order, Leaseweb and Customer also will provide the Data Subject(s) to which the Customer Data relates reasonable assistance with ad hoc redress mechanisms.
4. To the extent not prohibited by Applicable Law or order, Leaseweb promptly will notify Customer in the event Leaseweb receives any request or order from governmental authorities in the United States seeking disclosure of the Customer Data. Promptly following its receipt of any such notice, Customer will notify the Data Subject of the request or order to enable the Data Subject to seek information and an effective redress.

5. Leaseweb will take no action pursuant to U.S. Executive Order 12333. Additionally, Leaseweb has not created back doors or similar programming, or created or changed its business processes, in a manner designed to facilitate governmental authorities' access to Customer Data pursuant to FISA Section 702 or other national security process or EO 12333, and Leaseweb currently is under no legal obligation to do so.
6. To the extent not prohibited by law, Leaseweb will document: (i) the requests that Leaseweb receives from governmental authorities seeking disclosure of the Customer Data, (ii) Leaseweb's response (if any) to such requests, and (iii) whether Customer and the applicable Data Subjects to which the Customer Data pertains have been notified of such request/disclosure. Leaseweb also will publish a transparency report indicating the types of binding legal demands for the personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702.
7. Leaseweb will share Customer Data with a Subprocessor only if such sharing is permitted by other provisions of the DPA and the Subprocessor meets one of the following conditions:
    a. It processes the Customer Data only in the European Economic Area or another jurisdiction whose laws have been recognized by the European Commission as providing adequate protection for the Customer Data;
    b. It receives the Customer Data only in situations where technical safeguards (such as appropriate end-to-end encryption) eliminate the ability of the Subprocessor to understand the substance of the Customer Data;
    c. It has agreed to safeguards at least as protective as those set forth in this Annex 3; or
    d. the transfer to the Subprocessor meets another condition specified in then-current guidance issued by the European Data Protection Board or the Irish Data Protection Commission for permissible transfers of Customer Data to parties located in a jurisdiction whose laws have not been recognized by the European Commission as providing adequate protection.
8. Leaseweb will, with due regard to the state of the art, in accordance with the risk of the categories of data processed and the likelihood of attempts from governmental authorities to access it, provide additional technical safeguards for the Customer Data processed hereunder by (i) applying a series of physical, technical and security services that are compliant with the industry security standards, including ISO 27001, SOC1, HIPAA and PCI DSS, and (ii) implementing additional measures, including (without limitation) next generation firewalls, virus scanning software, full disk encryption, encrypted communication via SSL or VPN, splunk log management, monthly security awareness trainings for all employees, and access controls such as multi-factor authentication, Single Sign On, access on an as-needed basis, strong password controls, and restricted access to administrative accounts.
9. Leaseweb will adopt, and regularly review, internal policies to assess the adequacy of the technical and organizational measures it has in place to protect Customer Data that is transferred to or by it outside of the United Kingdom or the EEA and, to the extent not prohibited by Applicable Law or order, will use such additional measures as are required to

maintain an equivalent level of protection for the Customer Data to that guaranteed within the EU.

10. Leaseweb will promptly notify Customer if Leaseweb can no longer comply with the Standard Contractual Clauses or the clauses in this Annex 3.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name: Leaseweb USA, Inc.

Authorised Signature: Alexander Boost, CEO and President.