DATA PROTECTION ADDENDUM FOR CUSTOMERS

This Data Protection Addendum ("**Addendum**") dated _____ forms part of the Terms of Service ("**Terms**") between (i) Vultr Holdings Corporation, ("**Vultr**"), and (ii) _____, with a registered account email of _____, acting on its own behalf and in the name and on behalf its Affiliates collectively, "**Customer**", each being a "**Party**" and together the "**Parties**".

The Customer will be providing to Vultr Personal Data that is subject notably to GDPR and accordingly Customer is required to impose on Vultr specific Processing terms in relation to the Processing of that Personal Data. The Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Terms and references in this Addendum to the Terms are to the Terms as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

(a) "**Addendum Effective Date**" has the meaning given to it in section 2;

(a) "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either Customer or Vultr (as the context allows), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

(b) "**Customer Personal Data**" means any Personal Data that (i) Processed by Vultr (a) on behalf of Customer, or (ii) otherwise Processed by Vultr, in each case pursuant to or in connection with instructions given by Customer in writing, consistent with the Terms and (ii) subject to Data Protection Laws;

(c) "**Controller to Processor SCCs**" means the Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC set out in Decision 2010/87/EC as the same are revised or updated from time to time by the European Commission;

(d) "**Data Protection Laws**" means (i) Directive 95/46/EC and, from 25 May 2018, Regulation (EU) 2016/679 ("GDPR") together with applicable legislation implementing or supplementing the same or otherwise relating to the processing of Personal Data of natural persons, (ii) to the extent not included in sub-clause (i), the Data Protection Act 1998 of the United Kingdom, as amended from time to time, and including any substantially similar legislation that replaces the DPA 1998, and (iii) the national legislation of the Swiss Confederation on the protection of Data Subjects with regard to the processing of Personal Data and on the free movement of such data, as amended from time to time, and other data protection or privacy legislation in force from time to time in the Swiss Confederation; and

(e) "**Services**" means the services to be supplied by Vultr to Customer pursuant to the Terms.

1.2 The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process**" and "**Processor**" have the same meanings as described in the Data Protection Laws and cognate terms shall be construed accordingly.

1.3 Capitalized terms not otherwise defined in this Addendum shall have the meanings ascribed to them in the Terms.

2. Formation of this Addendum

The Parties agree that this Addendum comes into effect on May 25, 2018 (the "**Addendum Effective Date**").

3. Roles of the Parties

The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data, and as more fully described in **Annex [1]** hereto, Customer acts as a Controller and Vultr acts as a Processor.

The Parties expressly agree that Customer shall be solely responsible for ensuring timely communications to Customer's Affiliates who receive the Services, insofar as such communications may be required or useful in light of applicable Data Protection Laws to enable Customer to comply with such Laws.

4. Description of Personal Data Processing

In **Annex [1]** to this Addendum, the Parties have mutually set out their understanding of the details of the Processing of the Customer Personal Data to the extent Processed by Vultr pursuant to this Addendum, as required by Article 28(3) of the GDPR. Either Party may make reasonable amendments to **Annex [1]** by written notice to the other Party and as reasonably necessary to meet those requirements. **Annex [1]** does not create any obligation or rights for any Party.

5. Data Processing Terms

5.1 Customer shall comply with all applicable Data Protection Laws in connection with the performance of this Addendum. As between the Parties, Customer shall be solely responsible for compliance with applicable Data Protection Laws regarding the collection and processing of and transfer to Vultr of Customer Personal Data.

5.2 Vultr shall:

5.2.1 Process the Customer Personal Data solely on the documented instructions of Customer, for the purposes of providing the Services and as otherwise necessary to perform its obligations under the Terms including with regard to transfers of Customer Personal Data to a third country outside the European Union or an international organization (unless required by Union or Member State law to which Vultr is subject, in which case Vultr shall inform Customer, if applicable, of that legal requirement before such Processing, unless that law prohibits such information on important grounds of public interest); Vultr shall immediately inform Customer if, in Vultr's opinion, an instruction infringes applicable Data Protection Laws;

5.2.2 ensure that persons authorized to Process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

5.2.3 implement and maintain the technical and organizational measures set out in in **Annex [2]** hereto, which the Parties have mutually agreed pursuant to Article 32 of the GDPR, having regard to the assessment of the appropriate level of security for Customer Personal Data and the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access or damage to such Personal Data. Any amendment to such agreed measures

that is necessitated by a change in the types of Personal Data Processed, or the risks of Processing, shall be dealt with via an agreed change control process between Vultr and Customer;

5.2.4 be expressly and specifically authorized by Customer to engage another Processor to Process the Customer Personal Data ("**Sub-Processor**"), subject to Vultr's:

a. notifying Customer of any intended changes to its use of Sub-Processors by emailing notice of the intended change to Customer;
b. including data protection obligations in its contract with each Sub-Processor which are materially the same as those set out in this Addendum; and
c. remaining liable to the Customer for any failure by each Sub-processor to fulfil its obligations in relation to the Processing of the Customer Personal Data.

In relation to any notice received under section 5.2.4 a., the Customer shall have a period of 30 (thirty) days from the date of the notice to inform Vultr in writing of any reasonable objection to the use of that Sub-processor. The Parties will then, for a period of no more than 30 (thirty) days from the date of the Customer's objection, work together in good faith to attempt to find a commercially reasonable solution for the Customer which avoids the use of the objected-to Sub-Processor. Where no such solution can be found, Vultr may (notwithstanding anything to the contrary in the Terms) terminate the relevant Services immediately on written notice to the other Party, without penalty or indemnification ;

5.2.5 to the extent legally permissible, promptly notify Customer of any communication from a Data Subject regarding the Processing of Customer Personal Data, or any other communication (including from a supervisory authority) relating to any obligation under the Data Protection Laws in respect of the Customer Personal Data and, taking into account the nature of the Processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR. Customer acknowledges that Vultr has no knowledge of any data (including Personal Data) that Customer has stored . Customer agrees to pay Vultr for time and for out of pocket expenses incurred by Vultr in connection with the performance of its obligations under this Section 5.2.5;

5.2.6 notify Customer without undue delay of any Personal Data Breach involving Customer Personal Data, upon Vultr's becoming aware of such a Personal Data Breach, the notice to include all information reasonably required by Customer to comply with its obligations under the Data Protection Laws;

5.2.7 assist Customer with its obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the Processing and information available to Vultr. Customer acknowledges that Vultr has no knowledge of any data (including Personal Data) that Customer has stored pursuant to the Terms and therefore Customer is solely liable for assessing the adequacy of the Services for the Customer Personal Data]. Customer agrees to pay Vultr for time and for out of pocket expenses incurred by Vultr in connection with any assistance provided in connection with Articles 35 and 36 of the GDPR;

5.2.8 cease Processing the Customer Personal Data upon the termination or expiry of the Terms, and at Customer's option obligations either return or delete (including by

ensuring such data is in non-readable format) all copies of the Customer Personal Data Processed by Vultr, unless (and solely to the extent and for such period as) Union or Member State law requires storage of the Personal Data. Notwithstanding the foregoing or anything to the contrary contained herein, Vultr may retain Personal Data and shall have no obligation to return Personal Data to the extent required by applicable laws or regulations. Any such Personal Data retained shall remain subject to the obligations of confidentiality set forth herein; and

5.2.9 once per year during the term of the Terms, Vultr will provide to Customer, on reasonable notice, responses to cybersecurity and other assessments for the purpose of confirming Vultr's compliance with its obligations under this Addendum.

6. Transfers

Customer (as "data exporter") and Vultr (as "data importer"), with effect from the commencement of the relevant transfer, hereby enter into the Controller to Processor SCCs (*mutatis mutandis*, as the case may be) in respect of any transfer from Customer to Vultr (or onward transfer) where such transfer would otherwise be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address Data Protection Laws). Appendix 1 to the Controller to Processor SCCs shall be deemed to be prepopulated with the relevant sections of **Annex [1]** to this Addendum and the processing operations are deemed to be those described in the Terms. Appendix 2 to the Controller to Processor SCCs shall be deemed to be prepopulated with **Annex [2]** to this Addendum.

7. Indemnity

To the extent permissible by law, Customer shall indemnify and hold harmless Vultr against all (i) losses, (ii) third party claims, (iii) administrative fines and (iv) costs and expenses (including, without limitation, reasonable legal, investigatory and consultancy fees and expenses) reasonably incurred in relation to (i), (ii) or iii), suffered by Vultr and that arise from any breach by Customer of this Addendum or of its obligations under applicable Data Protection Laws.

8. Severability

The Parties agree that, if any section or sub-section of this Addendum is held by any court or competent authority to be unlawful or unenforceable, it shall not invalidate or render unenforceable any other section of this Addendum.

9. Precedence

The provisions of this Addendum are supplemental to the provisions of the Terms. In the event of any inconsistency between the provisions of this Addendum and the provisions of the Terms, the provisions of this Addendum shall prevail.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Terms with effect from the Addendum Effective Date.

_____ **("Customer")**	**Vultr ("Vultr")**
Signature _____	Signature Michael Nolan
	Michael Nolan
Name	Name
	VP of Finance
Title	Title
	May 21, 2018
Date Signed	Date Signed

Annex [1]: Description of Processing of Customer Personal Data

This Annex includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of the Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in in Sections 1.1 and 3.1 of the Terms.

The nature and purpose of the Processing of the Personal Data

The nature and purpose of the Processing of the Customer Personal Data are set out as described in Section 3.1 of the Terms.

The categories of Data Subject to whom the Customer Personal Data relates

The Customer is solely responsible for determining the categories of Data Subject to whom the Customer Personal Data relates, and for indicating to Vultr those categories. Vultr only stores such Data, or backs it up upon Customer demand.

The types of Customer Personal Data to be Processed

The Customer is solely responsible for determining the types of Personal Data to be Processed, and for indicating to Vultr those types. Vultr only stores such Data, or backs it up upon Customer demand.

The obligations and rights of Customer

The principal obligations and rights of Customer are set out in Sections 3, 5-9, and 12-22 of the Terms and in this Addendum.

Data exporter (as applicable)

Customer, which engages Vultr for the services specified in the Terms.

Data importer (as applicable)

Vultr, which provides the services to Customer pursuant to the Terms.

Processing operations (as applicable)

The personal data transferred will be subject to the following basic processing activities (please specify):

Vultr stores and backs up the data (including any Personal Data) that the Customer chooses to have hosted by Vultr.

Annex [2]: Technical and Organizational Measures

1. Vultr implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of personal data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

2. Vultr implements acceptable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (This includes telephones, database, backup, and application servers and their related hardware) where the personal data are processed or used. This includes establishing security areas, establishing access authorizations for employees and third parties, including the respective documentation, all access to the data centers where personal data are hosted is logged, monitored, and tracked, and the data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

3. Security of the network powering the Vultr Cloud is a critical component of our overall security objectives. The production data network is isolated from our corporate enterprise network in order to offer access only to staff members with legitimate business access needs.

4. The Vultr enterprise network is protected with protected IP space, isolation, firewalls and 2FA.

5. Access to Vultr Cloud Production network components is only permitted from a jump-box (bastion host) with audited user credentials located on the Enterprise network.

6. All devices that perform routing or switching of Vultr Cloud Production traffic are managed using templates with out-of-band audited change management tools. The templates are designed with default, limited, control plane ACL's to ensure access is highly limited. Additionally, non-routed IP space is implemented wherever possible to limit CPU exposure to Internet traffic. Encrypted access to these devices is only permitted from the bastion host. Central log collection is utilized for expedited troubleshooting.

7. The Vultr automation and hypervisor cluster security is enforced through strict firewall enforcement and limited access trusted engineers. System health is monitored from our 24x7x365 NOC through a variety of central logging tools, proactive monitoring, and internal portals alerts.

8. Our engineering team also manages critical patches centrally through internal repositories and follows industry-standard peer review practices to publish changes in a non-customer impacting fashion. Additionally, non-routed IP space is implemented wherever possible to limit CPU exposure to Internet traffic. Encrypted access to these devices is only permitted from the bastion host. Central log collection is utilized for expedited troubleshooting.