RACKSPACE DATA PROCESSING ADDENDUM

CONTRACT AMENDMENT

This Data Processing Addendum ("DPA") amends the agreement between the Rackspace entity ("Rackspace") and the supplier described therein ("Supplier") as described below. The DPA sets out additional duties and obligations of the Supplier with respect to its processing of Personal Data for the Services provided. Unless otherwise defined herein, any capitalized terms shall have the meaning given to them in the Agreement (as defined below).

1. DEFINED TERMS

1.1. The following terms shall have the following meanings in the DPA:

"Affiliate" means a member of the Rackspace group of companies (other than Rackspace) as appropriate;

"Adequate Country" shall mean: (i) a country within the European Economic Area; or (ii) a country or territory which is subject to a current finding of the European Commission that it ensures an adequate level of protection within the meaning of Applicable Data Protection Law;

"Agreement" means the agreement between Rackspace and the Supplier for the provision of the Services;

"Applicable Data Protection Law" means all applicable laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations in relation to data privacy, including but not limited to the EU General Data Protection Regulation ((EU) 2016/679);

"Client" means any legal entity which has entered into a contract for hosting services and/or other information technology services with Rackspace or its Affiliates;

"Controller", "Processor", "Data Subject", "Personal Data" and "Process" or "Processing" shall all have the meanings set out in Applicable Data Protection Law;

"Personal Data" means any Personal Data relating to Rackspace or its Affiliates (where Rackspace or its Affiliates act as Controller) and/or any Personal Data relating to the Client or the Client's end-users (where Rackspace or its Affiliates acts as a Processor) in relation to which the Supplier is providing the Services or which the Supplier may have access to from time to time in performing the Services and may include without limitation the categories of Personal Data set out in Annex 1 of the DPA;

"Services" means the services or support described in the Agreement; and


2. OBLIGATIONS OF SUPPLIER

2.1 To the extent that the Supplier Processes any Personal Data, for or on behalf of Rackspace and/or any Client in the course of providing the Services, it shall at its own cost and expense:
2.1.1 comply with the obligations that apply to it under Applicable Data Protection Law;

2.1.2 remain in scope with the subject matter of the Processing; the duration of the Processing (which shall be from the date of this DPA until the Agreement expires or terminates in accordance with its terms); the purpose of the Processing; the type of Personal Data Processed; and the categories of Data Subjects made available to the Supplier as part of the Services, including employees, contractors, individuals to whom we market, partners of Rackspace or its Clients or any of their end users or customers who are individuals (as detailed in Annex 1);

2.1.3 process Personal Data only on Rackspace’s documented instructions, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by EU or EU Member State law to which the Supplier is subject; in such a case, the Supplier shall inform Rackspace of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The Supplier shall immediately inform Rackspace if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law;

2.1.4 ensure that all Supplier personnel (including staff, agents and subcontractors) who the Supplier authorizes to Process Personal Data are subject to a strict duty of confidentiality, and the Supplier shall not permit any person to process Personal Data who is not under such a duty of confidentiality. The Supplier shall ensure that all such personnel process the Personal Data only as necessary for the purpose stated in Clause 2.1.2;

2.1.5 maintain and implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access. Such measures shall include (as a minimum) the security measures set out in Annex 2 and the appropriate technical and organisational measures to ensure a level of security appropriate to the risk including:

2.1.5.1 the pseudonymisation and encryption of Personal Data;

2.1.5.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

2.1.5.3 the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

2.1.5.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

2.1.6 immediately notify Rackspace and provide all necessary assistance in respect of any (i) request from a Data Subject to exercise any of her or his rights under Applicable Data Protection Law (including rights of access, correction, objection, erasure and data portability, as applicable), and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the processing of Personal Data;

2.1.7 immediately report to Rackspace any known or suspected breach of security that may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed ("Security Incident"), and provide to Rackspace all necessary information and cooperation as needed so that Rackspace can fulfil any data breach reporting
obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. The Supplier shall also further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Rackspace informed of all developments in connection with the Security Incident;

2.1.8 immediately inform Rackspace if the Supplier believes or becomes aware that its Processing of Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, and it shall provide Rackspace with all necessary assistance as Rackspace may require in order to conduct a data protection impact assessment and, if necessary, consult with the relevant data protection authority or authorities;

2.1.9 upon request, immediately delete or return all Personal Data in its possession or control, including existing copies thereof and any Personal Data subcontracted to a third party for Processing, except to the extent the Supplier is required by European Union or EU Member State law to store all or part of the Personal Data, in which case it shall isolate and protect such Personal Data from any further processing except to the extent required by such law;

2.1.10 maintain a record of all processing of Personal Data it carries out on behalf of Rackspace and make available to Rackspace all information necessary to demonstrate its compliance with this DPA or Applicable Data Protection Law and allow for and contribute to audits, including inspections conducted by Rackspace or other third party;

2.1.11 maintain an online listing or make available to Rackspace an up-to-date list of its subprocessors; impose written data protection terms on any subprocessor that processes Rackspace’s Personal Data that are no less restrictive than the terms of this DPA and Applicable Data Protection Law; remain liable for any breach of this DPA that is caused by an act, error or omission of its subprocessor. Rackspace may object to the appointment or replacement of a subprocessor by terminating its use of the affected Services for convenience upon giving written notice in the manner provided in the Agreement; and

2.1.12 agree that the Supplier's name, country of location and the Services and the function it performs for Rackspace may be included by Rackspace in any list of Processors or subprocessors maintained by Rackspace and made available to Clients, supervisory authorities or others.

2.2 **EU DATA TRANSFERS:** To the extent that EU data transfers occur, Supplier shall comply with the following:

2.2.1 **Privacy Shield.** For data transfers directly to the U.S. and any onward transfers, Rackspace adheres to both EU-U.S. and U.S.-Swiss Privacy Shield compliance frameworks. Notwithstanding Supplier’s certification status under these frameworks, and to the extent that EU or Swiss data transfers occur, the Supplier agrees to apply the same or greater level of protection as required by the Privacy Shield Principles (“Principles”) under the relevant Privacy Shield Framework. Details about the requisite Principles under these frameworks can be found at [https://www.privacyshield.gov](https://www.privacyshield.gov). If the Supplier is unable to meet these obligations at any time, then the Supplier must immediately notify Rackspace, cease all processing of EU or Swiss Personal Data, and adhere to the data transfer, deletion, or destruction protocol as set forth by Rackspace upon receipt of such notice.
2.2.2 **Standard Contractual Clauses.** For EU data transfers directly to countries other than the United States and Switzerland, that have not been recognized by the EU Commission as an Adequate Country, the Supplier shall implement EU Standard Contractual Clauses or other legally-valid, EU-approved data transfer mechanism, if applicable, in accordance with the notice provision set forth in the Agreement(s) and prior to such transfers.

2.2.3 In relation to the Standard Contractual Clauses, (for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection):

2.2.3.1 subject to clause 2.2.3.2, below, the sub-processor clauses are hereby incorporated by reference as though fully rewritten herein;

2.2.3.2 the Supplier agrees to comply with the clauses of the Standard Contractual Clauses that are applicable to sub-processors, these being clauses 1, 3, 5, 6, 7, 8(2), 8(3), 10, 11 and 12 and appendices 1 and 2 (which are attached to the DPA as Annexes 1 and 2 respectively) (the "**sub-processor clauses**"), for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. The sub-processor clauses are governed by the law of the member state in which the relevant Controller is established;

2.2.3.3 the Supplier agrees to comply with the obligations described in the sub-processor clauses even if Personal Data is processed in an Adequate Country;

2.2.3.4 where the sub-processor clauses contain any obligation to notify the "data exporter" (as such term is defined in the sub-processor clauses), such notification shall be made via Rackspace; and

2.2.3.5 the Supplier acknowledges that any Data Subject shall have the right to enforce the sub-processor clauses against the Supplier, in cases where both the data exporter and the data importer (as such terms are defined in the Standard Contractual Clauses) 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. The Supplier's liability shall be limited to its processing operations under the Agreement.

3. **GENERAL**

3.1 All other terms and conditions in the Agreement remain in full force and effect and are binding upon the parties.

3.2 In the event that there are any inconsistencies between this DPA and the Agreement, this DPA shall prevail as it relates to data protection.

3.3 Save as set out at clause 2, the provisions of the governing law clause of the Agreement shall apply to the DPA.
IN WITNESS WHEREOF the parties’ authorized signatories have duly executed the DPA on the date set out below. The DPA shall become effective on the date of the last signature and will thereafter form part of the Agreement.

<table>
<thead>
<tr>
<th>Rackspace Entity:</th>
<th>Supplier:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td>Signature:</td>
</tr>
<tr>
<td>Name and Title:</td>
<td>Name and Title:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
Annex 1

Data subjects

Personal Data transferred includes but is not limited to the following categories of Data Subjects:

- Prospects, customers, business partners and suppliers of the data exporter (who are natural persons);
- Employees or contact persons of data exporter’s prospects, customers, business partners and suppliers;
- Employees, agents, advisors, freelancers of data exporter; and
- Data exporter’s users authorised by the data exporter to use the Services.

Categories of data

The Personal Data transferred includes but is not limited to email, documents and other data in an electronic form as may be transmitted or stored by the data exporter in the context of the Services.

Special categories of data (if appropriate)

The Personal Data transferred may concern special categories of data as may be transmitted or stored by the data exporter in the context of the Services.

Processing operations

The Personal Data transferred will be subject to the following basic Processing activities (please specify):

Transfers are made for the performance of the Services by the Supplier.
Annex 2

Description of the technical and organizational security measures implemented by the Supplier

1. Defined Terms. The terms below shall have the meanings stated when used in this Annex 2. Terms not otherwise defined in this Annex 2 shall have the meaning stated in the Agreement.

“Information Technology Systems” means any physical or virtual device used to access, process, or store Secure Information; any software used to store or process Secure Information; and any communications infrastructure used to transmit Secure Information.

“Secure Information” means (i) information belonging to Rackspace which is subject to legislative or regulatory requirements, or protected by any means other than enforcement of a contract, including (but not limited to) any material, non-public information; trade secrets; information covered by the Payment Card Industry Data Security Standard; health or medical information of an individual; and information subject to privacy or data protection laws; and (ii) any information about, belonging to, or stored by a Rackspace customer.

“Strong Authentication” means the use of authentication mechanisms and methodologies that require a unique login and a Strong Password for each individual; maintain detailed access logs; require users to change passwords at first log-on; enforce regular password changes; store password files separately from application system data; visually obfuscate passwords as they are being entered; store and transmit passwords using Strong Encryption and hashing algorithms; and prohibit default, commonly used, or easily guessed passwords. Examples of Strong Authentication mechanisms and methodologies include digital certificates from approved Certificate Authorities, two-factor authentication, and one-time passwords.

“Strong Encryption” means the use of encryption technologies with key lengths of at least 256-bits Advanced Encryption Standard for symmetric encryption and 2048-bits for asymmetric encryption, whose strength provides reasonable assurance that it will protect the encrypted information from unauthorized access, and is adequate to protect the confidentiality and privacy of the encrypted information, and which incorporates a documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality of the keys and passwords used as inputs to the encryption algorithm. Insecure versions of Secure Sockets Layer and Transport Layer Security protocols, such as SSL 3.0 and TLS 1.0, are not strong cryptographic protocols.

“Strong Password” means a password comprised of no less than eight (8) characters and shall include at least one each of the following: uppercase letters, lowercase letters, numeric characters, and special characters.

“Supplier Personnel” means Supplier’s employees, officers, directors, members, managers, and others to whom Supplier gives access to Secure Information.

2. Best Practices and Guiding Principles. The following principles shall govern all use and disclosure of Secure Information by Supplier under this Agreement.

   i. **Minimal Standards.** Secure Information shall be treated with at least as much care and diligence as Confidential Information.

   ii. **Best Practices.** Supplier shall at all times follow industry best practices with regard to Secure Information.
iii. **Least Access; Limited Duration.** When disclosing Secure Information, Supplier shall grant the least amount of access required and for the limited duration such access is needed in order to meet Supplier's obligations under the Agreement. Logical access controls shall be based on the principles of least privilege and segregation of duties.

iv. **Greatest Protection.** As between the Agreement, this DPA, and applicable governing laws, Supplier's obligations with regards to protecting Secure Information are cumulative. To the extent there is a conflict which prevents Supplier from complying with the conflicting terms, Supplier shall comply with the terms providing the greatest protection for the Secure Information, Personal Data and Data Subjects allowed by law.

v. **Ultimate Responsibility.** Supplier must obtain written authorization from Rackspace before disclosing Secure Information to any third party. Supplier shall only disclose Secure Information to Supplier Personnel or authorized third parties who need to know the information, who have been made aware of the obligations herein, and who have entered into an agreement with Supplier that provides materially similar or better protections for the Secure Information as are provided under this DPA. Supplier shall be at all times responsible to Rackspace for the use and disclosure of the Secure Information by anyone to whom Supplier discloses the Secure Information.

vi. **Awareness and Training.** Supplier Personnel with access to the Secure Information must be provided with information security awareness training and correct information processing requirements prior to gaining access to the Secure Information and, thereafter, on a periodic basis (no less frequently than annually). Any third party to whom Supplier discloses Secure Information should have contractual obligations to provide such training and requirements to its own personnel.

vii. **Reasonable Cooperation.** Supplier shall comply with Rackspace's reasonable requests and instructions with regard to Secure Information including, at a minimum, fully and accurately responding to Rackspace's security questionnaire regarding Information Technology Systems and taking steps Rackspace may reasonably require to use such Information Technology Systems in a secure manner.

viii. **Background Screening.** To the extent allowed by applicable law, for US personnel, Recipient shall conduct a background screening of each individual to whom it gives access to Secure Information at the federal, state and county levels, including each county where the individual has lived for the past seven years (or other reasonable requirements that Rackspace may communicate to Supplier from time to time). For non-US personnel, Supplier shall use commercially reasonable efforts to meet the same criteria as established for US personnel, subject to general business practices in the respective country and industry, and further subject to reasonable availability of information and documentation. The screening must be performed by a reputable third-party screening service prior to the date that the individual is given access to Secure Information. Supplier shall not disclose Secure Information to an individual who has been found guilty of a felony offense or crime involving fraud, dishonesty, or moral turpitude.

3. **Documentation.** Supplier shall have documented policies and procedures which comply with the requirements of this Annex 2 and applicable industry standards to address the following:

i. the administration of information security throughout Supplier's organization, including definitions of information security roles, responsibilities, and accountability;
access control rules and permissions related to the Secure Information, which shall include a process for secure creation, modification, and deletion of user accounts with no less than annual audits of such access rights;

iii. the geographic location and governing jurisdiction of all Information Technology Systems;

iv. to the extent applicable, Supplier’s software development lifecycle process following industry best practices for secure coding methods which shall include, at a minimum, regular code reviews and validation checks prior to any release of software into a production environment;

v. general operating procedures related to the prevention, monitoring, and remediation of any unauthorized access, security breach, or computer virus or malware on any Information Technology System;

vi. disaster recovery related to Information Technology Systems and business continuity of Services provided to Rackspace;

4. Physical Security. Supplier shall take the additional precautions below with respect to the physical security of Secure Information in its possession.

i. Supplier shall maintain an asset inventory of Information Technology Systems which includes the designated owner and location. Supplier shall develop and implement an appropriate set of procedures for the labelling and handling of Secure Information.

ii. Any Information Technology System used to store or process Secure Information shall be located in a controlled access facility with physically secure perimeters, external entry points that protect against unauthorized access, and built to standards prescribed under applicable law (including, where applicable, ISO or IEC codes).

iii. Supplier shall restrict access to areas which store the Secure Information to authorized Supplier Personnel using reasonable access controls and authentication mechanisms.

iv. Access to areas which store the Secure Information must be monitored, recorded, and controlled with physical access rights reviewed no less than annually. Physical access logs shall be stored for a period of no less than one year.

v. Supplier Personnel and authorized visitors with access to facilities which store Secure Information must be issued with a unique identification card which must be worn visibly at all times.

vi. Supplier shall prohibit its personnel from copying any part of the Secure Information on to a device of any kind for use outside of Supplier’s controlled access facility.

vii. Specifically, but without limitation, Supplier Personnel shall not access Secure Information while located in any public place, or copy any Secure Information to any portable or physical media for use outside of the controlled access facility, including any laptop, mobile device, removable media, portable external drive, “thumb drive,” or similar media or technology.

5. Logical Security. Supplier shall follow industry best practices and take the additional precautions below with respect to the logical security of Secure Information in its possession.

i. As applicable, Supplier shall ensure any Information Technology System automatically locks or logs out when left unattended.
ii. Information Technology Systems shall be segregated as necessary and protected by a physical firewall with all ports blocked except those needed for specific Supplier applications, and Supplier shall take such other measures as are reasonable in light of the Secure Information to which it has access. Such additional measures may include, and Rackspace, in its sole discretion, may require: virus and malware scanning, intrusion detection and prevention technologies, managed secure patching practices, third party vulnerability testing, and virtual private networking or multi-factor authentication schemes.

iii. Information Technology Systems must be protected by and may only be accessed using Strong Authentication systems.

iv. Supplier shall encrypt Secure Information stored on any Information Technology System using Strong Encryption methods. If Supplier transfers any Secure Information via the internet or any untrusted network, it shall encrypt the Secure Information using Strong Encryption methods while in transit.

v. Supplier shall use cryptographic and hashing algorithm types, strength, and key management processes consistent with industry best practices.

vi. Supplier shall centrally manage access to any Information Technology System and implement an appropriate set of procedures for authorizing logical access to Secure Information that ensures access is appropriate according to the business function of Supplier personnel.

vii. As applicable, access to Information Technology Systems must be monitored, recorded, and controlled to a reasonable standard.

6. Cloud Services. No third party or Supplier-provided cloud services may be used to store, process, access, or transmit Secure Information unless such services meet all the requirements of this Annex 2.

7. Incident Management. Supplier shall notify Rackspace immediately (and in no event later than 24 hours) if it becomes aware of any access to or loss of Secure Information other than as authorized by this DPA and shall provide Rackspace with all information available to it, as permitted by law, that Rackspace may reasonably request in connection with any such incident. Notwithstanding the generality of the foregoing, Supplier shall provide the following within two (2) Business Days of Rackspace’s request following an incident: the complete results of any required background screening; signed copies of any written confidentiality obligations; a digital image of each individual to whom Supplier has given access to the Secure Information; and the access logs to the breached Information Technology System(s). Rackspace acknowledges that such information is the Confidential Information of Supplier as defined in the Agreement.

8. Audit Right. Supplier shall maintain, at no additional cost to Rackspace, in a reasonably accessible location, all records pertaining to its compliance with this Agreement and its Services provided to Rackspace under this Agreement. Rackspace may, at its sole expense, perform a confidential audit of such Supplier records referenced above and Supplier’s Information Technology Systems, during normal business hours and at such reasonable times as Rackspace and Supplier may determine. Records available for review shall exclude any records pertaining to Supplier’s other customers deemed proprietary and confidential and Supplier confidential and proprietary records not associated with this Agreement. Supplier agrees to cooperate fully with any such request or audit. Without limiting the foregoing, Supplier agrees that it will cooperate with any operational audit or certification process undertaken by Rackspace intended to evidence that Rackspace or a Rackspace customer meets hosting industry security standards (such as a Payment Card Industry Certification or applicable ISO
standards), International Standards for Assurance Engagements No. 3402, or Statement on Standards for Attestation Engagements No. 16 or equivalent standards applicable in the relevant jurisdiction.

9. **Breach.** Supplier's breach of this Annex 2 shall constitute a material breach of the Agreement. Rackspace may, at its option and without liability under the Agreement, suspend Supplier's access to the Secure Information during any period that the Supplier is not in compliance with this Annex 2, or any period during which Rackspace reasonably suspects that the Supplier is not in compliance with this Annex 2.

10. **Survival.** The terms of this Annex 2 survive expiration or termination of the Agreement for so long as Supplier has possession of or access to the Secure Information.