RACKSPACE GLOBAL DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is an addendum to the Agreement and addresses each party's compliance obligations under Applicable Data Protection Law. The DPA applies solely in respect of the provision of Services by Rackspace to Customer, where such Service provision involves the Processing of Customer Personal Data subject to Applicable Data Protection Law.

1. ADDITIONAL DEFINED TERMS.

"**Applicable Data Protection Law**" means any applicable privacy, data protection, or data security law or regulation applicable to a party's Processing of Customer Personal Data under the Agreement, including subordinate legislation, regulations, and binding guidance issued thereunder (in each case, as amended, adopted, or superseded from time to time).

"**Applicable SCCs**" means the standard contractual clauses or equivalent transfer mechanism approved or required under the relevant Applicable Data Protection Law for the transfer of Customer Personal Data to a region outside the applicable Prescribed Region, as identified in Schedule 3 (Jurisdiction Table).

"**Approved EU SCCs**" means the European Union standard contractual clauses pursuant to Commission Implementing Decision (EU) 2021/914.

"**Controller**" means an entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data (or equivalent term under Applicable Data Protection Law, including "Business" under US Privacy Laws).

"**Customer Audit**" means a review of the security of the Services conducted by Customer at its expense.

"**Customer Instructions**" means the Customer's instructions to Rackspace as its Processor as documented in the Agreement, together with the Customer's lawful and proper use of the Services.

"**Customer Personal Data**" means Personal Data Processed by Rackspace for Customer in relation to the Services.

"**Data Subject**" means the individual to whom Personal Data relates (or equivalent term under Applicable Data Protection Law, including "Consumer" under US Privacy Laws).

"**End-user**" means Customer's own customers or affiliates whose Personal Data is Processed by Rackspace through the provision to or use by Customer of the Services.

"**Personal Data**" means "personal data", "personal information", "personally identifiable information" or equivalent term as defined under Applicable Data Protection Law.

"**Prescribed Region**" means, with respect to any category of Customer Personal Data, a country, territory, or jurisdiction to which such data may be lawfully transferred without Transfer Protections under the Applicable Data Protection Law governing that data, as specified in Schedule 3 (Jurisdiction Table). Where Schedule 3 does not address a particular Applicable Data Protection Law, "Prescribed Region" means any jurisdiction recognized as providing adequate protection for personal data under that law.

"**Privacy Policy**" means the Rackspace Privacy Statement (presently found at the following URL: www.rackspace.com/information/legal/privacystatement), as periodically updated by Rackspace.

"**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data. For example, accessing, storing, transmitting, transforming, disclosing, and deletion.

© 2022 Rackspace US, Inc. - Global DPA - June 17, 2026 Revision OT# 50186

"**Processor**" means an entity that Processes Personal Data on behalf of the Controller (or equivalent term under Applicable Data Protection Law, including "Service Provider" under US Privacy Laws).

"**Security Incident**" means a breach of Rackspace's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Personal Data.

"**Sell**" and "**Share**" shall have the meanings given to each term under the CCPA and US Privacy Laws.

"**Sensitive Data**" means "sensitive data", "special categories of data", or equivalent term as defined under Applicable Data Protection Law.

"**Service Metadata**" means technical, operational, and usage data generated through Customer's use of the Services, including log data, performance metrics, configuration data, API calls, resource utilization statistics, and error reports. Service Metadata does not include Customer Data content.

"**SPP Terms**" means the Rackspace Security and Privacy Practice terms (presently found at the following URL: www.rackspace.com/information/legal/securitypractices), as periodically updated by Rackspace.

"**Sub-processor**" means a vendor that Rackspace has engaged to Process Customer Personal Data.

"**Sub-processor List**" means the Rackspace Authorized Sub-processors list (presently found at the following URL: www.rackspace.com/gdpr/subprocessors), as periodically updated by Rackspace.

"**Third Party Audit Report**" means a report resulting from Rackspace engaging qualified third party auditors to perform examinations and provide reports of its systems and services in accordance with: (i) the best practice recommendations of ISO 27002, for the purpose of auditing Rackspace's compliance with ISO 27001; (ii) SSAE 16 and ISAE 3402 compliance frameworks, and the AT 101 compliance framework (based upon select Trust Services Principles) and/or equivalent industry standards.

"**TOMs**" means the Rackspace Technical and Organizational Measures (presently found at the following URL: www.rackspace.com/information/legal/toms), as periodically updated by Rackspace.

"**Transfer Protections**" means transfer protection measures required under Applicable Data Protection Law to enable a lawful transfer of Customer Personal Data outside a Prescribed Region, as identified in Schedule 3 (Jurisdiction Table).

"**US Privacy Laws**" means the CCPA, VCDPA, ColPA, UCPA, CTDPA, and other comprehensive US state privacy laws, including regulations promulgated thereunder, each as amended or superseded. For the avoidance of doubt, US Privacy Laws excludes HIPAA.

2. DATA PROCESSING.

2.1. Processing Roles. Rackspace may act as Processor to Customer, where Customer may act either as Controller or Processor, with respect to Customer Personal Data. Rackspace may also act as a Sub-processor. Where Customer acts as Processor, Customer shall be responsible for all Controller obligations under this DPA; and Customer warrants that the Controller has appointed Customer as Processor to Process Personal Data of the Controller on the Controller's behalf. To the extent any Service Metadata (as defined in the Agreement) is considered Personal Data under Applicable Data Protection Law, Rackspace is the Controller of such data and shall Process such data in accordance with the Agreement and Applicable Data Protection Law. The details of Processing (the nature and purpose of processing of Personal Data, the type of Personal Data subject to the processing, and the duration of Processing) and the description of transfer are stated at Schedule 1.

2.2. Sub-processor Appointment. Rackspace may use Sub-processors to fulfil its obligations under the Agreement. Customer provides general authorization for Rackspace to engage Sub-processors to Process Customer Personal Data. Rackspace maintains an up-to-date Sub-processor List. Where required by Applicable Data Protection Law, Rackspace shall inform Customer of any addition to or change in Sub-processors by updating the Sub-processor List, or by providing written notice to Customer, prior to any new Sub-processor being authorized to Process any Customer Personal Data; and Customer may object to

Rackspace's appointment or replacement of a Sub-processor by giving written notice of termination of the affected Services in accordance with the termination for convenience provisions of the Agreement, within the seven (7) day period following the Sub-processor List update or notice of update (whichever is earlier). Customer's termination pursuant to this section 2.2 shall be Customer's sole and exclusive remedy for any objection to a new Sub-processor. Customer's notice of termination under this section 2.2 shall be ineffective if Rackspace notifies Customer prior to termination that the proposed appointment or replacement shall not be effective as to Customer.

2.3. Sub-processor Obligations. Rackspace shall impose contractual obligations on its Sub-processors (including confidentiality, data protection and data security) as required by Applicable Data Protection Law, including, where so required, imposing written data protection terms which are consistent with those in this DPA on any Sub-processor (taking into account the nature of the Services that require such sub-processing by the Sub-processor). Rackspace remains responsible for any acts or omissions of a Sub-processor that cause Rackspace to breach Rackspace's obligations under this DPA.

2.4. Processing under US Privacy Laws. To the extent that Rackspace's Processing of Customer Personal Data is governed by US Privacy Laws, this Section 2.4 applies. Customer discloses or otherwise makes available Customer Personal Data to Rackspace for the limited and specific purpose of Rackspace providing the Services to Customer in accordance with the Agreement and this DPA. Rackspace shall:

(A) not Sell or Share Customer Personal Data;

(B) (i) use Customer Personal Data only for the purpose of fulfilling its duties under the Agreement; and (ii) shall not retain, use, share or disclose Customer Personal Data to any third parties, or use Customer Personal Data for purposes outside of the direct business relationship between Rackspace and Customer or for any commercial purpose, except as permitted by the Agreement (including to perform the Services), otherwise required by law (including cooperating with law enforcement agencies where Rackspace reasonably and in good faith believes conduct or activity may violate applicable law), or upon the prior consent of Customer;

(C) not combine the Customer Personal Data which Rackspace receives from or on behalf of Customer, with Personal Data which Rackspace receives from or on behalf of another person or persons, or collects from Rackspace's own interaction with the Data Subject; provided that Rackspace may combine Customer Personal Data to perform any business purpose permitted by US Privacy Laws (including without limitation to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity); and

(D) comply with the applicable sections of US Privacy Laws. Customer agrees that Rackspace shall meet its obligation to provide at least the same level of privacy protection to Customer's account-related Personal Data that it would apply to equivalent Personal Data processed by Rackspace in its own corporate IT systems by implementing the measures set out in section 5.3. Rackspace shall notify Customer after Rackspace makes any determination that Rackspace cannot meet its obligations under the US Privacy Laws, or that Rackspace's use of Customer Personal Data is inconsistent with this DPA and such use cannot be reasonably cured; and in such circumstances Customer may stop Processing Customer Personal Data at any time by ceasing use of the Services.

2.5. Controller Activities. Rackspace is a Controller of account-related data, Service Metadata, and Aggregated Data, Customer billing information, and Customer's Personal Data as specified in Rackspace's Privacy Notice. This DPA does not limit or prohibit Rackspace from acting in that capacity.

2.6. Services Operations. Customer acknowledges that Rackspace employs artificial intelligence and machine learning technologies as an integral component of service delivery for operational purposes including infrastructure management, security monitoring, and service optimization. Such processing is necessary for the performance of the Services and does not require separate consent. To the extent any such processing

constitutes service improvement rather than direct service delivery, Rackspace relies on its legitimate interest in maintaining efficient operations and improving service quality, subject to appropriate safeguards.

3. DOCUMENTED CUSTOMER INSTRUCTIONS.

3.1. The Customer Instructions constitute Customer's complete and final documented instructions regarding Rackspace's Processing of Customer Personal Data. Where required by Applicable Data Protection Law to which Rackspace is subject, Rackspace shall Process Customer Personal Data in accordance with lawful Customer Instructions. Additional instructions outside the original scope of the Customer Instructions require prior written agreement between the parties, including any additional fees payable by Customer to Rackspace for carrying out such instructions.

3.2. Customer represents and warrants that: (i) Customer has complied and will comply with Applicable Data Protection Law; (ii) Customer has obtained and will obtain and continue to have, during the term, all necessary rights, lawful bases, authorizations, consents, and licenses for the Processing of Customer Personal Data as contemplated by the Agreement; (iii) Rackspace's Processing of Customer Personal Data in accordance with the Agreement will not cause Rackspace to violate or breach Applicable Data Protection Law or cause a breach of any agreement or obligations between Customer and any third party; and (iv) Customer is responsible for determining whether the Services are appropriate for the Processing of Customer Personal Data under Applicable Data Protection Law. Customer shall ensure that it has all necessary consents, notices and other requirements in place to enable lawful Processing of the Customer Personal Data by Rackspace for the duration and purposes of this Agreement.

3.3. Without prejudice to Customer's obligations under section 3.2 and where required by Applicable Data Protection Law to which Rackspace is subject, Rackspace shall inform Customer if, in its reasonable opinion, a Customer Instruction infringes Applicable Data Protection Law and shall, without liability, be entitled to stop Processing Customer Personal Data in accordance with such infringing instruction. The parties acknowledge and agree that a failure or delay by Rackspace to identify that a Customer Instruction infringes Applicable Data Protection Law shall not cause Rackspace to be in breach of this DPA or its obligations under the Agreement nor shall it relieve Customer from its liability under the DPA.

4. CROSS-BORDER TRANSFERS.

4.1. General Transfer Restriction. Rackspace shall not transfer any Customer Personal Data outside of the applicable Prescribed Region unless Transfer Protections are in place as required by the Applicable Data Protection Law governing that data. Subject to such Transfer Protections, Customer agrees that Customer Personal Data may be transferred to and Processed in countries where Rackspace or its Sub-processors maintain facilities or personnel (which may be outside of the country or other jurisdiction in which Customer has chosen to store Customer Personal Data), as necessary for Rackspace to fulfill its obligations under the Agreement.

4.2. Applicable SCCs. Where the Applicable Data Protection Law requires the use of standard contractual clauses or an equivalent transfer mechanism for transfers outside the applicable Prescribed Region, the parties agree to comply with the Applicable SCCs identified in Schedule 3 (Jurisdiction Table) as though set out in full in this DPA, with Customer acting as data exporter and the Rackspace contracting entity acting as data importer (or equivalent roles under the Applicable SCCs). Schedule 4 sets out the description of the transferred Personal Data and the details of the parties, Processing, and applicable annexes. Any third-party beneficiary rights set out in the Applicable SCCs shall be solely applicable to those Applicable SCCs. The Applicable SCCs shall not apply where the Rackspace contracting entity is located in the applicable Prescribed Region (even where the Rackspace contracting entity subsequently transfers Customer Personal Data to an Affiliate outside of a Prescribed Region).

4.3. SCC Conflict Resolution. If there is a conflict between the body of this DPA and any Applicable SCCs, the Applicable SCCs will prevail solely with respect to the Processing of Customer Personal Data governed by the Applicable Data Protection Law under which those Applicable SCCs were adopted. For the avoidance of

doubt, the Applicable SCCs are subject to the rights, obligations, limitations, and exclusions of liability under the Agreement, to the extent permitted by the governing Applicable Data Protection Law.

4.4. Interpretive Provisions for Non-EU SCCs. In respect of Processing governed by an Applicable Data Protection Law other than the EU GDPR, the Applicable SCCs (where based on or derived from the Approved EU SCCs) shall not be interpreted in a way that conflicts with rights provided to Data Subjects under the governing Applicable Data Protection Law; and where the country from which the Customer Personal Data originated is not a member state of the EU, references in the Approved EU SCCs to: (a) the "European Union," the "EU," a "Member State," or "one of the EU Member States" shall refer to the applicable country from which the relevant Customer Personal Data originated; (b) Regulation (EU) 2016/679 shall refer to the Applicable Data Protection Law in the applicable country; and (c) "supervisory authority" shall refer to the competent regulator as set out in Schedule 3 (Jurisdiction Table), Field E.

4.5. Transfer Impact Responsibilities. For the purposes of any transfer impact assessment required under Applicable SCCs (e.g., Section III, Clause 14 of the Approved EU SCCs, or equivalent provisions under other Applicable SCCs), Rackspace and Customer acknowledge and agree that, as between the parties, Customer is responsible for: (i) assessing the laws of the country to which Customer transfers the Customer Personal Data; and (ii) determining whether or not the transfer meets the applicable requirements. Where Rackspace (as data importer) provides information to Customer (acting as data exporter) for assisting Customer in Customer's assessment, such information is provided on an "as is" basis for informational purposes only. Rackspace (as data importer) shall not be liable for any losses suffered by Customer in connection with its assessment.

4.6. Cessation of Adequacy. Where a transfer is made under Transfer Protections to a region that subsequently becomes a Prescribed Region, such that the Transfer Protections are no longer required under Applicable Data Protection Law, the relevant Transfer Protections shall automatically expire. Conversely, in the event that the jurisdiction in which the Rackspace contracting entity is established ceases to be designated as a Prescribed Region, transfers of Customer Personal Data by Customer to Rackspace in that jurisdiction shall become subject to Section 4.2.

4.7. Data Subject Communications. Where requested by Rackspace, Customer shall be responsible for issuing such communications to Data Subjects and other Controllers, as are required for Rackspace to comply with its obligations under any Applicable SCCs.

4.8. General. Rackspace shall comply with the obligations of the data importer or Sub-processor as appropriate under Applicable Data Protection Law.

5. SECURITY OF DATA PROCESSING.

5.1. Rackspace shall ensure that all Rackspace personnel (including staff, agents and subcontractors) Rackspace authorizes to Process Customer Personal Data are subject to duties of confidentiality.

5.2. Notwithstanding anything to the contrary in the Agreement, Customer remains the primary system and account administrator and is responsible for the integrity, security, maintenance and appropriate protection of Customer Personal Data including by: (i) selecting, purchasing, and properly configuring appropriate Services; (ii) implementing adequate controls to maintain appropriate security, protection and deletion of Customer Personal Data (which shall include end-to-end encryption in transit and at rest, and logical access measures); (iii) ensuring that Rackspace is not provided with any access to Customer Personal Data (including, without limitation, any protected health information as described in section 10 below), except as otherwise explicitly set out in the Agreement; and (iv) using data integrity controls to allow Customer to restore the availability of Customer Personal Data in a timely manner (which shall include routine backups and archiving of Customer Personal Data in an environment separate from the Customer Configuration). Rackspace makes available a number of security controls that Customer may elect to purchase as part of the Services. Rackspace will only back up data to the extent purchased by Customer as part of the Services, and stated on a Service Order.

5.3. Subject to section 5.2, Rackspace shall implement technical and organizational measures (including but not limited to the pseudonymization and encryption of Customer Personal Data; ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; ability to restore availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing) as appropriate to its Processing of Customer Personal Data and the risk of a Security Incident, and having regard to the state of technological development and cost of implementation. Customer is responsible for making an independent determination as to whether the technical and organizational measures implemented by Rackspace meet Customer's requirements, including any of its security obligations under Applicable Data Protection Law. Customer agrees that the appropriate technical and organizational measures are the measures to be implemented by Rackspace and set out in the SPP Terms and TOMs, together with such security controls made available by Rackspace and which the Customer elects to purchase as part of the Services; and that these measures meet Customer's needs with respect to Customer's security obligations under Applicable Data Protection Law, and Rackspace's obligations under Applicable Data Protection Law and this section 5.3.

6. PRIVACY IMPACT ASSESSMENTS, PRIOR CONSULTATION & AUDIT.

6.1. Privacy Impact Assessments & Prior Consultation. Upon Customer's reasonable request, and taking into account the nature of the Processing, Rackspace shall provide reasonable assistance to Customer in fulfilling Customer's data protection impact assessment and prior consultation obligations under Applicable Data Protection Law, by providing the reports provided under the SPP Terms and information pursuant to any Customer Audit under section 6.26.2 or information provision obligations under section 6.3, provided that Customer cannot reasonably fulfill such obligations independently with help of available documentation. Customer shall reimburse Rackspace for all non-negligible costs Rackspace incurs in performing its obligations under this section 6.1.

6.2. Audit. The audit provisions in any Applicable SCCs shall be subject to this section 6.2. Rackspace is regularly audited by independent third-party auditors. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with Rackspace, Rackspace will supply a summary copy of relevant Third-Party Audit Report(s) to Customer, so Customer can verify Rackspace's compliance with the audit standards against which it has been assessed, and this DPA. Only to the extent Customer cannot reasonably satisfy Rackspace's compliance with this DPA through review of such Third-Party Audit Reports, or where required by Applicable Data Protection Law or a regulatory authority, Rackspace agrees to permit Customer to perform a Customer Audit no more than once in any 12 month period, and upon not less than sixty (60) days' prior written notice from Customer. Any Customer Audit must: (i) be conducted during Rackspace's regular business hours; (ii) be at Customer's expense; (iii) be subject to reasonable confidentiality controls; (iv) be carried out by Customer's internal or external auditors who have entered into a non-disclosure agreement with Rackspace; (v) avoid disrupting Rackspace operations and be conducted strictly in accordance with Rackspace's security policies and procedures, and industry best practices; and (vi) restrict its findings to only information relevant to Customer. The parties must mutually agree on the scope of the review, prior to the date of the Customer Audit. The parties must mutually agree on any findings or subsequent remediations. Customer Audits must be limited in scope to the security of that portion of the Customer Configuration processing Customer Personal Data within Rackspace operated data centers, which are not covered by the Third-Party Audit Reports or SOC reports. Customer Audits exclude data related to other customers and Third-Party Services.

6.3. Information. To the extent required by Applicable Data Protection Law, upon Customer's reasonable request and at Customer's expense, Rackspace shall provide information reasonably necessary to demonstrate Rackspace's compliance with its obligations under this DPA, provided that Rackspace is not required to provide any information or documentation that (i) would cause it to breach any confidentiality obligations; (ii) could, in its reasonable opinion, compromise its information security measures; or (iii) relates to other customers or Rackspace's proprietary business information. Such right may be exercised no more than once every twelve (12) months.

7. SECURITY INCIDENT HANDLING.

7.1. Notification. Rackspace shall notify Customer without undue delay of any Security Incident of which Rackspace becomes aware, either by providing notice in accordance with the notice provisions of the Agreement or, where it is not practicable to do so, by posting the notice online. Such initial notice will include, to the extent reasonably available to Rackspace at the time of notification, information reasonably necessary for Customer to comply with its own notification obligations under Applicable Data Protection Law, which Rackspace may supplement as additional information becomes available. Rackspace shall have no obligation to notify Customer of any Security Incident that Rackspace reasonably determines does not present a material risk of harm to the affected Data Subjects, or trigger notification obligations under Applicable Data Protection Law, except as otherwise specifically set out as part of the Services in the Agreement. Rackspace's notification of or assistance with respect to any Security Incident shall not be construed as an acknowledgment by Rackspace of any fault or liability with respect to such Security Incident. Nothing in this section shall require Rackspace to disclose information that would compromise the security of Rackspace's systems, violate applicable law, or prejudice any law enforcement or regulatory investigation.

7.2. Assistance. Upon Customer's request and taking into account the nature of the Processing and the information available to Rackspace, Rackspace shall assist Customer by providing information reasonably necessary for Customer to meet its Security Incident notification obligations under Applicable Data Protection Law. All such assistance shall be at Customer's expense. Rackspace shall make reasonable efforts to identify the cause of the Security Incident and mitigate the effects to the extent within Rackspace's reasonable control. Rackspace's remediation and mitigation obligations shall be limited to Security Incidents arising from Rackspace's breach of its security obligations under the Agreement.

8. DATA SUBJECT RIGHTS. Taking into account the nature of the Processing, Rackspace shall provide reasonable and timely assistance to Customer, by appropriate technical and organizational measures and insofar as reasonably possible, to enable Customer to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law in respect of Customer Personal Data. Rackspace offers Customer certain self-service controls and tools through which Customer may fulfill its obligations to Data Subjects. Where Rackspace receives such requests directly from a Data Subject, Rackspace shall redirect such Data Subject to Customer or forward such requests to Customer. Customer is solely responsible for responding to such requests, and Rackspace shall have no obligation to respond to any Data Subject directly in respect of Customer Personal Data. Customer retains control over and primary responsibility for Customer Personal Data for the purposes of responding to Data Subject requests.

9. RETURN OR DELETION OF CUSTOMER DATA. The Services provide Customer with controls that Customer may use to retrieve, correct or delete Customer Personal Data prior to expiry or termination of the Agreement. Following expiry or termination of the Agreement, upon Customer's instruction, Rackspace shall delete all Customer Personal Data that Customer has not deleted using the aforementioned controls. Notwithstanding the foregoing, Rackspace may retain Customer Personal Data as required by law or good industry practice or in accordance with its standard backup or record retention policies, provided that, in either case, Rackspace will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and not further Process it except as required by applicable law.

10. HIPAA. Customer acknowledges that Rackspace is not a business associate or subcontractor (as defined in 45 CFR § 160.103) under HIPAA (and its implementing regulations as amended from time to time), and that the Services are not designed or intended for the storage or processing of protected health information ("PHI") (as defined in 45 CFR § 160.103). Customer represents and warrants that it shall not store, transmit, or process PHI in or through a Service, or otherwise provide PHI to Rackspace, unless the parties have first entered into a fully executed Business Associate Agreement ("BAA") under which Rackspace agrees to act as a business associate with respect to such PHI and the relevant Services. In the absence of such a BAA, Customer shall have no right to use the Services in connection with PHI, and Rackspace shall bear no liability arising from Customer's failure to comply with this section.

11. MODIFICATION REQUIRED BY LAW. Notwithstanding anything to the contrary in the Agreement, Rackspace also may amend this DPA as required to comply with any Applicable Data Protection Law by publishing a revised DPA on Rackspace's website. All updates made will be effective on the earlier of: (i) 90 days following publication

by Rackspace on its website, (ii) the effective date otherwise dictated by operation of the Agreement, or (iii) the effective date as required to comply with Applicable Data Protection Law.

12. LIABILITY. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the "Limitations on Damages" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. Rackspace's and its Affiliates' total liability for all claims from the Customer and all of its Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including its Schedules.

SCHEDULE 1
DETAILS OF PROCESSING / DESCRIPTION OF TRANSFER

Categories of Data Subjects whose personal data is transferred	The Data Subjects may include Customer's customers, employees, suppliers, and End-users.
Categories of personal data transferred by Customer or any End-user	Such Customer Personal Data as Customer provides to Rackspace in connection with the Services.
Sensitive Data transferred (if applicable) and applied restrictions or safeguards	Such limited Customer Personal Data that constitutes Sensitive Data as Customer provides to Rackspace in connection with the Services.
The frequency of the transfer	On a continuous basis, the frequency of which is determined by Customer.
Nature of the processing / processing operations	Rackspace processes Customer Personal Data as a data processor solely to provide the Services as documented in the Agreement. The scope of processing includes AI-enabled operations necessary for service delivery, security, optimization, and improvement. Customer's documented instructions are deemed to include any processing necessary for Rackspace to fulfill its obligations under the Agreement.
Purpose(s) of the data transfer and further processing	The purpose of the Processing is the provision of the Services to Customer and any resolution of technical issues provided for in the Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Until the expiration or termination of the Agreement, unless otherwise agreed in writing by Rackspace and Customer.
For transfers to (sub-) processors, subject matter, nature and duration of the processing	The nature and purpose of the Processing by Sub-processors is the provision of the Services to Customer, as provided for in the Agreement; and the duration is until the expiration or termination of the Agreement.

SCHEDULE 2
TECHNICAL AND ORGANIZATIONAL MEASURES

Rackspace is responsible for the technical and organizational measures set out in this DPA, and in the Agreement, including the SPP Terms and the TOMs. Customer is responsible for implementing and maintaining privacy protections and security measures set out in the Agreement, including for components that Customer provides or controls.

© 2022 Rackspace US, Inc. - Global DPA - June 17, 2026 Revision OT# 50186

SCHEDULE 3
JURISDICTION TABLE

Instructions for Use. Where Customer Personal Data is subject to an Applicable Data Protection Law listed in a jurisdiction entry below, the corresponding fields (A–F) apply to such data. Where a jurisdiction is not listed, the general provisions of this DPA apply, and "Prescribed Region" and "Transfer Protections" have the default meanings in Section 1.

3.1 European Union — EU GDPR.

A. Applicable Data Protection Law	Regulation (EU) 2016/679 (General Data Protection Regulation) and its respective national implementing legislations, including as implemented in non-EU member states in the EEA.
B. Prescribed Region	EEA member states and any region in respect of which a valid adequacy decision has been issued by the European Commission.
C. Applicable SCCs / Transfer Mechanism	Approved EU SCCs (Commission Implementing Decision (EU) 2021/914), Module 2 (C2P) or Module 3 (P2P) as applicable. Clause 7 (docking) applies solely for Affiliates. Clause 9, Option 2 (general written authorization).
D. Governing Law of SCCs	Laws of the Netherlands.
E. Supervisory Authority	Where Customer is established in the EEA: supervisory authority of that member state. Where Customer is not established in the EEA: Dutch Data Protection Authority (Autoriteit Persoonsgegevens).
F. Jurisdiction-Specific Requirements	None beyond core DPA. See Schedule 4, Section 4.5 for EU SCC-specific mechanical provisions.

3.2 United Kingdom — UK GDPR.

A. Applicable Data Protection Law	The EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, and the Data Protection Act 2018.

© 2022 Rackspace US, Inc. - Global DPA - June 17, 2026 Revision OT# 50186

B. Prescribed Region	The UK and any region recognized as adequate under the UK GDPR.
C. Applicable SCCs / Transfer Mechanism	Approved EU SCCs (Module 2 (C2P) or Module 3 (P2P) together with the UK International Data Transfer Addendum (template Addendum B.1.0, ICO, 2 February 2022). References to EU/Member State construed as references to UK. References to Regulation 2016/679 construed as references to UK GDPR.
D. Governing Law of SCCs	Per UK International Data Transfer Addendum.
E. Supervisory Authority	Information Commissioner's Office (ICO).
F. Jurisdiction-Specific Requirements	SCCs shall not be interpreted in a way that conflicts with UK GDPR data subject rights. See Schedule 5 for the UK International Data Transfer Addendum.

3.3 Switzerland — Swiss DP Law.

A. Applicable Data Protection Law	Swiss Federal Act on Data Protection of 19 June 1992 (FADP), as amended, superseded, or replaced, including by the revised version of 25 September 2020, and the Ordinance to the Federal Act on Data Protection.
B. Prescribed Region	Switzerland and any region recognized as adequate under the Swiss DP Law.
C. Applicable SCCs / Transfer Mechanism	Approved EU SCCs with Swiss-specific interpretive provisions per Section 4.4 of this DPA. References to EU/Member State construed as references to Switzerland. References to Regulation 2016/679 construed as references to Swiss DP Law.
D. Governing Law of SCCs	Laws of the Netherlands (or as otherwise required by Swiss DP Law).
E. Supervisory Authority	Swiss Federal Data Protection and Information Commissioner (FDPIC).

F. Jurisdiction-Specific Requirements	SCCs shall not be interpreted in a way that conflicts with Swiss DP Law data subject rights.

3.4 United States — US Privacy Laws.

A. Applicable Data Protection Law	The California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA); the Virginia Consumer Data Protection Act (VCDPA); the Colorado Privacy Act (ColPA); the Utah Consumer Privacy Act (UCPA); the Connecticut Data Privacy Act (CTDPA); and other comprehensive US state privacy laws, including regulations promulgated thereunder, each as amended or superseded. Excludes HIPAA.
B. Prescribed Region	N/A (no cross-border transfer mechanism required under US Privacy Laws).
C. Applicable SCCs / Transfer Mechanism	N/A.
D. Governing Law of SCCs	N/A.
E. Supervisory Authority	N/A.
F. Jurisdiction-Specific Requirements	Section 2.4 of this DPA applies in full. Key obligations: no Sell or Share of Customer Personal Data; purpose limitation to the direct business relationship; prohibition on combining Customer Personal Data with data received from other sources except as permitted by US Privacy Laws; notification if Rackspace determines it cannot meet its obligations under US Privacy Laws.

3.5 Kingdom of Saudi Arabia — KSA PDPL.

A. Applicable Data Protection Law	The Personal Data Protection Law (PDPL) issued by Royal Decree No. (M/19) dated 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH, and implementing regulations thereunder.

B. Prescribed Region	Those regions or entities deemed to have an "appropriate level of protection" pursuant to KSA PDPL.
C. Applicable SCCs / Transfer Mechanism	KSA Standard Contractual Clauses for Personal Data Transfer, Version 1.0, September 2024 (KSA SCCs). All general clauses (Clauses 1 through 13) apply to all transfers. The Second Template applies solely where Customer is the Controller and Rackspace is the Processor. The Third Template applies solely where Customer is the Processor and Rackspace is the Sub-processor.
D. Governing Law of SCCs	Per KSA SCCs.
E. Supervisory Authority	Saudi Data and AI Authority (SDAIA) / National Data Management Office (NDMO).
F. Jurisdiction-Specific Requirements	(a) If signing of a copy of this DPA (or the KSA SCCs) becomes a requirement of KSA PDPL (as reasonably determined by Rackspace), Customer shall in a timely manner sign a copy of this DPA (or the KSA SCCs), retroactively effective to the original incorporation date, as directed by Rackspace. (b) For purposes of the KSA SCCs, the Appendix Information set forth in Schedule 4 (including the List of Parties and Description of Transfer) applies to transfers of KSA Personal Data. (c) Restrictions and/or safeguards applicable to Sensitive Data are as set forth in Schedule 2.

3.6 Brazil — LGPD.

A. Applicable Data Protection Law	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), as amended.
B. Prescribed Region	Brazil and any regions recognized as providing an adequate level of protection by the Autoridade Nacional de Proteção de Dados (ANPD).
C. Applicable SCCs / Transfer Mechanism	ANPD-approved Standard Contractual Clauses (when finalized and published) or alternative transfer mechanism under Article 33 of the LGPD.
D. Governing Law of SCCs	Per ANPD SCCs (when available).

E. Supervisory Authority	Autoridade Nacional de Proteção de Dados (ANPD).
F. Jurisdiction-Specific Requirements	(a) DPO appointment obligations (if applicable under the LGPD) rest with Customer as Controller. (b) Rackspace will cooperate with ANPD requests directed to it in its capacity as Processor.

3.7 Vietnam — PDP Law / Decree 13.

A. Applicable Data Protection Law	The Law on Personal Data Protection (Law No. 91/2025/QH15, effective 1 July 2026), and Decree No. 13/2023/ND-CP on Personal Data Protection (to the extent it remains in effect), and implementing regulations thereunder.
B. Prescribed Region	Vietnam (for purposes of data localization requirements, if applicable).
C. Applicable SCCs / Transfer Mechanism	Cross-border transfer impact assessment dossier filed by Customer with the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention, A05). Rackspace shall provide reasonable assistance to Customer in preparing such dossier upon Customer's request and at Customer's expense.
D. Governing Law of SCCs	N/A.
E. Supervisory Authority	Ministry of Public Security (MPS), Department of Cybersecurity and High-Tech Crime Prevention (A05).
F. Jurisdiction-Specific Requirements	(a) Customer is solely responsible for filing the cross-border transfer impact assessment dossier with the MPS as required under the applicable law. (b) Customer is solely responsible for compliance with any data localization requirements applicable to Customer Personal Data. (c) Customer is solely responsible for any mandatory registration of data processing activities with the MPS, including processing of sensitive personal data and cross-border transfers.

3.8 United Arab Emirates — UAE PDPL.

A. Applicable Data Protection Law	Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, and implementing regulations thereunder.
B. Prescribed Region	The UAE and any regions recognized as providing an adequate level of protection under the UAE PDPL and its implementing regulations.
C. Applicable SCCs / Transfer Mechanism	Adequate safeguards as approved by the UAE Data Office (when implementing regulations are finalized and published). Until such regulations are finalized, transfers shall be conducted in accordance with the transfer provisions of the UAE PDPL as applicable.
D. Governing Law of SCCs	Per applicable UAE regulations (when finalized).
E. Supervisory Authority	UAE Data Office.
F. Jurisdiction-Specific Requirements	Customer is solely responsible for registration with the UAE Data Office if required under the UAE PDPL or its implementing regulations.

3.9 India — DPDPA.

A. Applicable Data Protection Law	The Digital Personal Data Protection Act, 2023, and rules promulgated thereunder by the Central Government.
B. Prescribed Region	India and any regions not designated as restricted for transfers by notification of the Central Government.
C. Applicable SCCs / Transfer Mechanism	As prescribed by Central Government rules (when finalized and published).
D. Governing Law of SCCs	Per applicable Central Government rules (when finalized).

E. Supervisory Authority	Data Protection Board of India.
F. Jurisdiction-Specific Requirements	(a) Customer is solely responsible for compliance with consent and notice requirements under the DPDPA. (b) Rackspace shall provide reasonable assistance to Customer in responding to requests from data principals exercising their rights under the DPDPA, in accordance with Section 8 of this DPA.

SCHEDULE 4
SCC APPENDIX INFORMATION

This Schedule contains the appendix information required by the Approved EU SCCs and is incorporated by cross-reference into all Applicable SCCs identified in Schedule 3 that require analogous appendix information (e.g., KSA SCCs).

4.1 List of Parties.

	Data Exporter	**Data Importer**
Entity	Customer	Rackspace contracting entity under the Agreement, where not located in a Prescribed Region
Address	The address Customer designates on Customer's account	19122 US 281, Suite 127, San Antonio, TX 78258, United States
Contact person	The individual(s) Customer designates as contact(s) on Customer's account	Chief Privacy Officer, privacy@rackspace.com
Activities relevant to the data transferred	The receipt of Services provided on or behalf of Rackspace as provided for in the Agreement	The provision of Services by or behalf of Rackspace as provided for in the Agreement
Signature and date	Customer's acceptance and date of acceptance of the Service Order constitutes signature and date herein	Rackspace's acceptance and date of acceptance of the Service Order constitutes signature and date herein
Role	Controller or Processor	Processor or Sub-processor

4.2 Description of Transfer. As set forth in Schedule 1, Section 1.1.

4.3 Competent Supervisory Authority. As specified in Schedule 3 (Jurisdiction Table), Field E, for the applicable jurisdiction.

4.4 Technical and Organizational Measures. As set forth in Schedule 2.

4.5 EU SCC-Specific Provisions. For the purpose of the Approved EU SCCs:

© 2022 Rackspace US, Inc. - Global DPA - June 17, 2026 Revision OT# 50186

(a) **Clause 8** (Data protection safeguards) shall be construed by reference to: Section 3.1 of this DPA for the purposes of Clause 8.1 (Instructions); Sections 6.2 and 6.3 of this DPA for the purposes of Clause 8.9 (Documentation and compliance); and Section 9 of this DPA for the purposes of Clause 8.5 (Duration of processing and erasure or return of data).

(b) **Clause 9, Option 2** (general written authorization for sub-processors) applies, and the time period for informing the data exporter of any changes to the Sub-processor List shall be the notice period set out in Section 2.2 of this DPA.

(c) **Clause 17** (governing law): notwithstanding anything to the contrary in the Agreement, and unless otherwise required by law or the UK International Data Transfer Addendum, the Approved EU SCCs (only) shall be governed by the laws of the Netherlands.

(d) **Clause 18** (choice of forum and jurisdiction): notwithstanding anything to the contrary in the Agreement and unless otherwise required by law or the Applicable SCCs, any dispute arising from the Approved EU SCCs shall be subject to the jurisdiction of, and resolved by, the courts of the Netherlands.

SCHEDULE 5
UK INTERNATIONAL DATA TRANSFER ADDENDUM

This Schedule is required by the ICO's prescribed template format and cannot be collapsed into the Jurisdiction Table.

Part 1: Tables

Table 1: Parties.

Start date	The effective date of the Agreement.	
The Parties	**Exporter** (who sends the Restricted Transfer):	**Importer** (who receives the Restricted Transfer):
Parties' details	Full legal name: Customer's name as designated in the Customer's account. Main address: The address Customer designates on Customer's account. Official registration number: The official registration number designated in the Customer's account, if any.	Full legal name: The Rackspace contracting entity under the Agreement. Main address: 19122 US 281, Suite 127, San Antonio, TX, 78258, United States. Official registration number: 4377687.
Key Contact	Full Name (optional): Job Title: The job title Customer designates on Customer's account, if any. Contact details including email: The email address Customer designates on Customer's account.	Full Name (optional): Job Title: Chief Privacy Officer. Contact details including email: 19122 US 281, Suite 127, San Antonio, TX, 78258, United States; privacy@rackspace.com.

Table 2: Selected SCCs, Modules and Selected Clauses.

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: the version of the Approved EU SCCs valid and in force as of the start date set out in Table 1.

Table 3: Appendix Information. "Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in Schedule 4.

© 2022 Rackspace US, Inc. - Global DPA - June 17, 2026 Revision OT# 50186

Table 4: Ending this Addendum when the Approved Addendum Changes.

Ending this Addendum	Which Parties may end this Addendum as set out in Section 19 of this Addendum: ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses. Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.