RACKSPACE SUPPLIER DATA PROCESSING ADDENDUM ("DPA") (ONLINE)

This Rackspace Supplier Data Processing Addendum (**"DPA"**) amends the Agreement (as defined below) between the contracting Rackspace entity and, as applicable, its Affiliates ("**Rackspace**") and the supplier or vendor ("**Supplier**") as identified within the Agreement (each a "**party**" and together the "**parties**"). This DPA is effective as of the effective date of the agreement between the parties into which it is incorporated by reference. The DPA sets out additional duties and obligations of Supplier with respect to its role as a Processor or sub-processor of Rackspace Personal Data. Unless otherwise defined herein, any capitalized terms shall have the meaning given to them in the Agreement. Rackspace may amend this Addendum at any time and at its sole discretion. Any changes will be effective upon the posting of such changes on the Rackspace website, and Supplier is responsible for regularly reviewing the website and informing itself of all applicable changes or notices. SUPPLIER'S CONTINUED PROVISION OF PRODUCTS OR SERVICES AFTER RACKSPACE'S POSTING OF ANY CHANGES SHALL CONSTITUTE SUPPLIER'S ACCEPTANCE OF SUCH CHANGES OR MODIFICATIONS.

1. DEFINED TERMS. The following terms shall have the following meanings in the DPA:

1.1. "**Affiliate**" means Rackspace Technology Global, Inc. and any entity that is directly or indirectly controlled (by more than 50% of the voting interests) by Rackspace Technology Global, Inc. As used in this definition, "Control" means the right to control more than 50% of the voting interests of the entity.

1.2. "**Agreement**" or "**Supplier Agreement**" means the agreement between Rackspace and Supplier for the provision of Services, including but not limited to any executed or click-through agreements.

1.3. "**Applicable Data Protection Law**" means all applicable data privacy, data protection or data security laws, rules, and regulations and applicable court rulings related to the provision or receipt of the Services provided by Supplier, including, but not limited to: (i) the EU GDPR; (ii) the UK GDPR; (iii) the Swiss DP Law; (iv) the Personal Data Protection Law of the Kingdom of Saudi Arabia ("KSA") 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, ("KSA PDPL" or "PDPL") (v) US privacy and security laws, including but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 et seq ("CCPA"); the Virginia Consumer Data Protection Act, Va. Code, 59.1-571 et seq ("VCDPA"); the Colorado Privacy Act, Col. Rev. Stat. § 6-1-1301 et seq ("ColPA"); the Utah Consumer Privacy Act S.B. 227, 2022 Gen. Assemb., Reg. Sess. (Utah 2022) ("UCPA"); and the Connecticut Data Privacy Act S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022) ("CTDPA"); or (vi) any subordinate legislation and regulation amendment or implementing such laws.

1.4. "**Controller**" means an entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data under Applicable Data Protection Law, and shall include "Business,"as defined under CCPA.

1.5. "**Customer**" means any legal entity which has entered into a contract with Rackspace or its Affiliates, for receipt of hosting services and/or other information technology services provided by Rackspace or its Affiliates.

1.6. "**Data Subject**" means the individual to whom Personal Data relates under Applicable Data Protection Law. For the avoidance of doubt, "Data Subject" includes "Consumer," as defined under the CCPA.

1.7. "**De-identified Data"** means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual and qualifies as "de-identified data" or a similar term under Applicable Data Protection Law.

1.8. "**EEA**" means the European Economic Area.

1.9. "**EEA Personal Data**" means Rackspace Personal Data to which the EU GDPR is applicable or was applicable prior to its Processing by Supplier.

1.10. "**EU**" means the European Union.

1.11. "**EU GDPR**" means (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and the free movement of that data, and repealing Directive 95/46/EC (General Data Protection Regulation); (ii) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of Personal Data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, (iii) any subordinate legislation and regulation implementing Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, in each case including as implemented in non-EU member states in the EEA.

1.12. "KSA Personal Data" means Rackspace Personal Data to which the KSA PDPL is applicable or was applicable prior to its Processing by Supplier.

1.13. "**Personal Data**" means "personal data", "personal information", "personally identifiable information" or such equivalent term, in each case as defined under Applicable Data Protection Law. Personal Data also includes "Personal Information," which is any information: (a) that identifies or can be used to identify, contact or precisely locate the person to whom such information pertains; or (b) from which identification or contact information of an individual person can be derived.

1.14. "**Prescribed Region**" means a country, territory or jurisdiction to which Rackspace Personal Data may be lawfully transferred without Transfer Protections, including: (i) for EEA Personal Data, any EEA member state and any region in respect of which a valid adequacy decision has been issued by the European Commission; (ii) for Swiss Personal Data, Switzerland and any region recognized as adequate under the Swiss DP Law; (iii) for UK Personal Data, the UK and any region which is recognized as adequate under the UK GDPR and (iv) for KSA Personal Data, the KSA and any region which is recognized as adequate under the KSA PDPL.

1.15. "**Process**" or "**Processing**" means the access, disclosure, transfer, storage, collection, recording, organization, structuring, adaptation or alteration, retrieval, consultation, deletion, combination, destruction, disposal, or other use of information or as defined by Applicable Data Protection Law.

1.16. "**Processor**" means an entity that Processes Personal Data on behalf of the Controller. For the avoidance of doubt, "Processor" shall also include "Service Provider," as the term is defined by the CCPA or Applicable Data Protection Law.

1.17. "**Rackspace Personal Data**" means any Personal Data relating to or provided by Rackspace or its Affiliates, Customers or Customer's end-users (including where Rackspace or its Affiliates act as Controller or Processor) in relation to which Supplier is providing the Services or which 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 Section 3 of Exhibit 1 of the DPA or Exhibit 2).

1.18. "**Rackspace Systems"** shall mean any Rackspace file computing system, database, server, website, application or networked environment or domain, including, without limitation, all development, quality assurance, and production environments.

1.19. "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 Applicable Data Protection Law; and (ii) any information about, belonging to, or stored by a Rackspace customer. Supplier shall not disclose Secure Information except as reasonably required to comply with the terms, obligations, and purpose of the Agreement.

1.20. "**Security Incident**" has the meaning provided for at Section 4.7 (Security Reporting) of this DPA.

1.21. "**Services**" means the products, services or support described in the Agreement.

1.22. "**Standard Contractual Clauses**" or "**SCCs**" means: (i) the European Commission standard contractual clauses adopted under, and set out in the annex of, Commission Implementing Decision (EU) 2021/914 as of 4 June 2021 ("**Approved EU SCCs**"); and (ii) in respect of UK Personal Data, the UK International Data Transfer Addendum and (iii) in respect of KSA Personal Data, the Saudi Data and AI Authority (SDAIA) standard contractual clauses adopted under, and set out in Article (29) of the PDPL and provisions of the Regulation on the Transfer of Personal Data Outside the Kingdom ("Approved KSA SCCs") appended to this DPA as Exhibit 2.

1.23. "Sub-processor", "subprocessor" or "subcontractor" means any third party (including any Supplier affiliate) authorized by Supplier to receive and Process any Rackspace Personal Data exclusively for the purpose of carrying out the Services.

1.24. "**Supervisory Authority**" means a governmental authority or regulator with authority under Applicable Data Protection Law over all or any part of the provision or receipt of the Services or the Processing of Personal Data pursuant to this DPA.

1.25. "**Swiss DP Law**" means the data protection laws of Switzerland, including the Swiss Federal Act on Data Protection of 19 June 1992 (FADP), as amended superseded, or replaced, including by the revised version of the Federal Act on Data Protection of 25 September 2020.

1.26. "Swiss Personal Data" means Rackspace Personal Data to which the Swiss DP Law is applicable or was applicable prior to its Processing by Supplier.

1.27. "**Transfer Protections**" means transfer protection measures required to enable a transfer to be made in compliance with Applicable Data Protection Law, including as applicable the recipient having: (i) achieved Binding Corporate Rules (as defined in Applicable Data Protection Law) authorization in accordance with Applicable Data Protection Law; (ii) executed Standard Contractual Clauses adopted or approved by the European Commission, or recognized in the UK, as applicable; (iii) executed Standard Contractual Clauses adopted or approved by the Supervisory Authority under the KSA PDPL or (iii) in place an alternative mechanism that complies with Applicable Data Protection Law for the transfer of Rackspace Personal Data to the applicable region.

1.28. "**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under: (i) the UK European Union (Withdrawal) Act 2018; and (ii) the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020 and the Data Protection Act 2018.

1.29. "**UK Personal Data**" means Rackspace Personal Data to which the UK GDPR is applicable or was applicable prior to its Processing by Supplier.

1.30. "**UK International Data Transfer Addendum**" (or, when used in this DPA, the "**Addendum**") means the Approved Addendum (as defined in Part 2 of Section 4 to Exhibit 1 to this DPA), incorporating the version of the Approved EU SCCs set out in table 2 of Section 4 to Exhibit 1 to this DPA (to which, notwithstanding anything to the contrary in this DPA, the Addendum shall be deemed

to be appended for the purposes of this DPA) and the Mandatory Clauses of the Addendum (as set out in Part 2 of Section 4 to Exhibit 1 to this DPA , and terms used in Section 4 of Exhibit 1 to this DPA and not defined in this DPA shall have the meanings set out in the Mandatory Clauses).

2. STATUS AND ROLES OF THE PARTIES.

2.1. Where Rackspace has entered into the Agreement for itself and for and on behalf of its Affiliates, all references to "Rackspace" in this DPA (and in respect of the Standard Contractual Clauses, where these apply) shall be construed as reference to the applicable Rackspace Affiliate(s) whose Rackspace Personal Data is Processed by Supplier pursuant to the Agreement.

2.2. Rackspace may act as a Controller or Business, or it may act as a Processor or Service Provider. Supplier therefore acknowledges that it may act as a Processor, Sub-processor or Service Provider to Rackspace. In certain situations, Rackspace is obligated contractually and/or under Applicable Data Protection Law to flow down relevant data protection related obligations to its appointed sub-processors. All obligations placed on Processors in this DPA shall apply to Supplier regardless of whether Supplier acts as a Processor or sub-processor.

3. NATURE OF THE PERSONAL DATA. The nature, purpose and subject matter of Supplier's Processing activities performed as part of the Services are set out in the Agreement and detailed at Exhibit 1 hereto.

4. SUPPLIER OBLIGATIONS. Supplier certifies that it understands its restrictions and obligations set forth in this DPA. The Processing instructions to which Supplier is bound and agrees to adhere to, including the nature and purpose of the Processing, are set forth below in Exhibit 1 or Exhibit 2. To the extent that Supplier Processes any Rackspace Personal Data for or on behalf of Rackspace and/or any Customer in the course of providing the Services, it shall at its own cost and expense, comply with the following:

4.1. Compliance with Law. Supplier shall comply with the obligations that apply to it under Applicable Data Protection Law and will provide the same level of privacy protection as required of the Supplier under Applicable Data Protection Law. Supplier, upon the request of Rackspace, shall reasonably make available to Rackspace information in its possession necessary to demonstrate the Supplier's compliance with the obligations under Applicable Data Protection Law.

4.2. Data Processing Obligations

(A) In-scope Processing. Supplier shall only Process Rackspace Personal Data for the purposes of providing the Services or as otherwise instructed by Rackspace in writing in accordance with Section 4.2 (B) of this DPA and shall remain within the scope of permitted Processing as detailed in Exhibit 1 or Exhibit 2.

(B) Documented Instruction. Supplier shall Process Rackspace Personal Data only on Rackspace's documented instructions, including with regard to transfers of Personal Data to a country outside the applicable Prescribed Region or an international organization. Notwithstanding the foregoing, Supplier may also Process Rackspace Personal Data where required to do so by laws to which Supplier is subject, but only to the extent permitted by the Applicable Data Protection Law that applies to the relevant Rackspace Personal Data. Where such Processing is required by laws to which Supplier is subject, Supplier shall inform Rackspace of the applicable legal requirement as soon as possible and before Processing, unless that law prohibits such information on important grounds of public interest. Supplier shall immediately inform Rackspace if, in its reasonable opinion, an instruction breaches Applicable Data Protection Law. For the avoidance of doubt, Supplier will not Process Rackspace Personal Data outside of the direct business relationship between Rackspace and Supplier.

(C) De-Indentification. When Supplier acts as a Processor, it shall not re-identify Rackspace's De-identified Data without the prior consent of Rackspace.

4.3. Confidentiality. Supplier shall ensure that all Supplier personnel (including staff, agents and subcontractors) who Supplier authorizes to Process Rackspace Personal Data are subject to a strict duty of confidentiality in respect of the Rackspace Personal Data, and Supplier shall not permit any person to Process Rackspace Personal Data who is not under such a duty of confidentiality. Supplier shall ensure that all such personnel Process the Rackspace Personal Data only as necessary for the purposes stated.

4.4. Security. Supplier shall comply with the Rackspace Supplier Secure Information Addendum (SSIA) found at www.rackspace.com/information/legal/SSIA. Rackspace may update the language, requirements, or applicability of the SSIA at any time, or require changes to Supplier's information security policies and requirements to meet new industry standards, regulations, or Rackspace requirements. All updates will be effective upon posting of such changes on the Rackspace website unless a shorter period is required to meet requirements of Applicable Data Protection Law. Supplier should refer regularly to the Rackspace website to review the current terms.

4.5. Technical and Organizational Measures. Taking into account the context of Processing, Supplier shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Supplier shall maintain and implement appropriate technical and organisational measures to protect Rackspace Personal Data and/or Secure Information including protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Such measures shall include (as a minimum) the security measures set out in Section 3 of Exhibit 1 or Exhibit 2. Such measure shall ensure a level of security appropriate to the risk, including but not limited to:

(A) the pseudonymisation and encryption of Personal Data;

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

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

(D) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing;

(E) measures for user identification and authorization;

(F) measures for the protection of data during transmission;

(G) measures for the protection of data during storage;

(H) measures for ensuring physical security of locations at which Rackspace Personal Data are Processed;

(I) measures for ensuring events logging;

(J) measures for ensuring system configuration, including default configuration;

(K) measures for internal IT and IT security governance and management;

(L) measures for certification/assurance of processes and products;

(M) measures for ensuring data minimization;

(N) measures for ensuring data quality;

(O) measures for ensuring limited data retention;

(P) measures for ensuring accountability; and

(Q) measures for allowing data portability and ensuring erasure.

4.6. Assistance. Supplier shall immediately (and in any event within 48 hours) notify Rackspace and provide all necessary assistance to Rackspace (or, if requested by Rackspace, the relevant Customer, where applicable) in respect of any (i) request from a Data Subject or Consumer 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) other correspondence, enquiry or complaint received from a Data Subject, Consumer, Supervisory Authority or other third party in connection with the Processing of Rackspace Personal Data or Rackspace's obligations under Applicable Data Protection Law. Supplier shall not respond to any such request or correspondence without Rackspace's prior written instructions.

4.7. Security Reporting. Supplier shall immediately (and in any event within 12 hours) report to Rackspace any known or suspected breach of security that may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed ("**Security Incident**"); and provide to Rackspace or, if requested by Rackspace, the relevant Customer 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. 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.

4.8. Ongoing Compliance. Supplier shall immediately inform Rackspace if Supplier can no longer comply with the technical and organizational measures required by Section 4.5 of this DPA, or 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 or, if requested by Rackspace, the relevant Customer may require in order to conduct a data protection impact assessment and/or transfer impact assessment and, if necessary, consult with the relevant Supervisory Authority or Supervisory Authorities.

4.9. Termination and Deletion. Upon request or upon termination, Supplier shall immediately delete or (at Rackspace's option) return in a commonly used data format all Rackspace Personal Data or Rackspace Information in its possession or control, including existing copies thereof and any Rackspace Personal Data or Rackspace Information subcontracted to a third party for Processing; unless laws to which Supplier is subject requires Supplier to store all or part of the Rackspace Personal Data (to the extent only that this ongoing storage is permitted by the Applicable Data Protection Law that applies to the relevant Rackspace Personal Data), in which case it shall isolate and protect such Rackspace Personal Data from any further Processing except to the extent required by such law.

4.10. Records. Supplier shall maintain a record of all Processing of Personal Data it carries out on behalf of Rackspace.

4.11. Sub-processors. Supplier may use Sub-processors to Process Rackspace Personal Data provided the conditions set out in this Section 4.11 are met. Supplier shall notify Rackspace of any Sub-processors in writing or maintain an online listing or make available to Rackspace upon request an up-to-date list of its Sub-processors (the "**Sub-processor List**"). Supplier shall:

(A) impose written data protection terms on any Sub-processor that Processes Rackspace Personal Data that are no less restrictive than the terms of this DPA and Applicable Data Protection Law and which require it to Process any Rackspace Personal Data only to the extent necessary to provide the Services (and for no other purpose);

(B) remain liable for any breach of this DPA that is caused by an act, error or omission of its Sub-processor;

(C) provide 60 days' prior notice by email to legalnotice@rackspace.com to Rackspace of any addition of a new Sub-processor to the Sub-processor List or replacement (including details of the jurisdiction in which the new Sub-processor processes Rackspace Personal Data), thereby giving Rackspace the opportunity to object to such changes prior to the engagement of the Sub-processor(s); and

(D) in the event that Rackspace objects in writing to Supplier's proposed use of such new Sub-processor, use reasonable efforts to stop a proposed Sub-processor from Processing Rackspace Personal Data without adverse impact on the Services. If Supplier determines that it cannot stop the Processing with adverse impact, it shall notify Rackspace of such determination. Upon receipt of such notice, Rackspace may terminate this Agreement without penalty or liability whatsoever (other than for charges due and owing to Supplier under the Agreement for Services supplied prior to such termination), such termination effective immediately upon giving notice of such termination to Supplier. Supplier shall promptly refund Rackspace any pre-paid charges for the period following the effective date of termination.

4.12. Sub-processor List. Supplier agrees that 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 sub-processors maintained by Rackspace and made available to Customers, Supervisory Authorities or others.

5. INTERNATIONAL DATA TRANSFERS.

5.1. Authority. Rackspace authorizes Supplier and its Sub-processors to make international data transfers of Rackspace Personal Data in accordance with this DPA provided that all such transfers are in accordance with this DPA and Applicable Data Protection Law.

5.2. International data transfers by Supplier. Supplier shall not transfer any Rackspace Personal Data outside of a Prescribed Region unless it has taken steps to ensure Transfer Protections are in place.

Upon request, Supplier will provide the following information to Rackspace in respect of transfers of EEA Personal Data, KSA Personal Data, Swiss Personal Data and/or UK Personal Data outside of a Prescribed Region made by Supplier:

(A) the transfer impact assessment made by Supplier in relation to the transfers;

(B) a summary of the access laws and practices that were assessed in respect of the transfers;

(C) a summary of the contractual, technical and organizational measures put in place in respect of the transfers; and

(D) to the extent not prohibited by law, details of the number of legally binding requests that the relevant data importer has received from a public authority in the relevant third country in each 12 month period over the last 24 months.

5.3. International data transfers by Rackspace to Supplier. Where Supplier is Processing EEA Personal Data and/or Swiss Personal Data and/or UK Personal Data and/or KSA Personal Data outside of a Prescribed Region without alternative Transfer Protections, each party agrees to comply with the obligations set out in the Standard Contractual Clauses as though they were set out in full in this DPA with Rackspace acting as data exporter and Supplier acting as data importer. Exhibit 1 (or as applicable Exhibit 2) to this DPA sets out the details of the: parties; Processing; Annexes and applicable modules

of the Approved EU SCCs, the Approved KSA SCC"s (and the details to be specified in the applicable modules or templates); and the UK International Data Transfer Addendum.

In respect of Processing by the Supplier of UK Personal Data and/or Swiss Personal Data, the Standard Contractual Clauses shall not be interpreted in a way that conflicts with rights provided to Data Subjects under the UK GDPR or Swiss DP Law and where the country in which Rackspace is established (or from where the EEA Personal Data, Swiss Personal Data or UK 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", an "EU Member State" or "one of the EU Member States" shall refer to the applicable country in which the Rackspace is established or from which the relevant Rackspace Personal Data originated;

(B) Regulation (EU) 2016/679 shall refer to the Applicable Data Protection Law in the country in which Rackspace is established or from which the relevant Rackspace Personal Data originated; and "supervisory authority" shall refer to the competent data protection supervisory authority as set out in Exhibit 1.

5.4. Prescribed Region Designation. In the event that the jurisdiction in which Supplier is established ceases to be designated as a Prescribed Region under the Applicable Data Protection Law of the EEA, the UK, Switzerland or KSA (as applicable), transfers of EEA Personal Data, KSA Personal Data, Swiss Personal Data and/or UK Personal Data (as applicable) by Rackspace to Supplier in that jurisdiction shall be subject to Section 5.3 of this DPA. Where a transfer of Rackspace Personal Data 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, where requested or agreed by Rackspace, Supplier agrees to terminate the relevant Transfer Protections.

5.5. Additional country requirements. Without prejudice to Sections 5.3 to 5.4 of this DPA, if Supplier at any time Processes Rackspace Personal Data originating in any country which restricts the Processing, export, or use of the relevant Rackspace Personal Data outside that originating country, Supplier will: (i) on Rackspace's instructions, take such actions (including implementing Transfer Protections) and execute such agreements as may be necessary under Applicable Data Protection Law in the originating country to legitimize any Processing by, or transfer to, Supplier of the Rackspace Personal Data; and (ii) ensure an adequate level of protection for the relevant Personal Data.

5.6. General. In the event that any competent judicial or supervisory authority holds that a data transfer mechanism relied on by the Parties under this Section 5 is invalid, or any competent judicial or supervisory authority requires transfers of Rackspace Personal Data made pursuant to such mechanism to be suspended, then Rackspace may, at its discretion, require Supplier to cease Processing Personal Data, or co-operate with it to facilitate use of an alternative transfer mechanism. Where Applicable Data Protection Law contains any obligation on the applicable data importer to notify the data exporter, Supplier shall make such notification to Rackspace. Supplier shall comply with the obligations of the data importer or sub-processor as appropriate under Applicable Data Protection Law. If signing of a copy of this DPA and/or the KSA SCCs becomes a requirement of Applicable Law (as reasonably determined by Rackspace), then Supplier shall in a timely manner sign of a copy of this DPA including any necessary SCC's or supporting material, retroactively effective to the original incorporation date, as directed by Rackspace.

6. AUDIT RIGHT. Supplier shall allow for, contribute to, and reasonably cooperate with Rackspace or Rackspace's designated assessor in its reasonable assessments of the Supplier's policies and technical and organizational measures in support of the obligations under Applicable Data Protection Law using an appropriate and industry-accepted control standard or framework and assessment procedure. Alternatively, the Supplier may arrange for a qualified and independent assessor to conduct, at least annually and at the Supplier's expense, the aforementioned assessment, using an appropriate and industry-accepted control standard or framework and assessment procedure for such assessments. Supplier shall provide a report of such assessment to Rackspace upon request. Supplier will also reasonably provide

information to Rackspace necessary to enable Rackspace to conduct and document any data protection assessments as required by Applicable Data Protection Law. Supplier shall maintain, at no additional cost to Rackspace, in a reasonably accessible location, all records pertaining to: (i) its compliance with this DPA and Applicable Data Protection Law; and (ii) its Services provided to Rackspace under the Agreement. Rackspace may, at its sole expense, perform (or require a third party to perform) a confidential audit and/or inspection, 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. 18 or equivalent standards applicable in the relevant jurisdiction. Supplier shall comply with all reasonable requests or directions by Rackspace to enable it to verify that Supplier, its personnel and any Sub-processor engaged by Supplier are in full compliance with Applicable Data Protection Law and this DPA and take such remedial actions as are reasonably required by Rackspace following such audit or inspection.

7. 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 the technical and organizational measures required by Section 4.5 of this DPA.

8. CCPA. If Supplier is Processing Personal Information within the scope of the CCPA, notwithstanding anything to the contrary in the Agreement, Supplier will process Rackspace Personal Data only to deliver services as instructed and permitted by Rackspace, in compliance with Applicable Data Protection Law, collect that Personal Data approved by Rackspace, not sell or share (as those terms are defined in the CCPA) and not process Rackspace Personal Data for any other purpose, including for a commercial purpose other than the business purposes set forth in this DPA and the direct business relationship between Rackspace and Supplier, unless Rackspace has provided its prior written agreement or otherwise required by Applicable Data Protection Law. In addition, Supplier will not retain, use, or share such data with any Third Party (as defined in CCPA) without the prior written consent of Rackspace except as required by the Agreement, this DPA, or Applicable Data Protection Law. Supplier grants Rackspace the right to take reasonable and appropriate steps to ensure that Supplier uses Rackspace Personal Data that it collected pursuant to the Agreement in a manner consistent with Rackspace's obligations under Applicable Data Protection Law. Supplier grants Rackspace the right, upon notice, to take reasonable and appropriate steps to stop and remediate the use of Rackspace Personal Data that is inconsistent with this DPA. Supplier shall refrain from combining Personal Data received from Rackspace with Personal Data (1) received from, or on behalf of, one or more entities to which it is a Processor; (2) collected from Rackspace's own interactions with the Data Subject; or (3) of opted-out Data Subjects which Rackspace receives from or on behalf of Rackspace with Personal Data which Supplier receives from or on behalf of another person or persons. If Supplier at any time determines that it can no longer meet its obligations under this DPA or Applicable Data Protection Law, Supplier shall notify Rackspace after Supplier makes such determination. Supplier shall cooperate with Rackspace, including but not limited to, providing documentation to Rackspace verifying that Supplier no longer retains or uses Rackspace Personal Data of Data Subjects who have made a valid request to delete with Rackspace.

9. INCIDENT MANAGEMENT. Supplier shall reasonably assist Rackspace in meeting obligations in relation to the security of Processing of Personal Data and in relation to the notification of a Security Incident. Without prejudice to Section 4.7, in the event of a Security Incident, Supplier shall provide the following within 48 hours of Rackspace's request: 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 Rackspace Personal Data; and the access logs to the breached information technology system(s) (and Rackspace acknowledges that such information is the Confidential Information of Supplier as defined in the Agreement).

10. CO-OPERATION WITH SUPERVISORY AUTHORITIES.

10.1. Unless Rackspace notifies Supplier that Supplier will be responsible for handling a particular communication or correspondence with a Supervisory Authority or a Supervisory Authority requests in writing to engage directly with Supplier, Rackspace will handle all communications and correspondence relating to Rackspace Personal Data and the provision or receipt of the Services. Supplier shall assist and support Rackspace in Rackspace's handling of communications and correspondence with the Supervisory Authority.

10.2. Where Supplier interacts directly with a Supervisory Authority in accordance with Section 10.1 of this DPA, Supplier shall do so in an open and cooperative way at its own expense and in consultation with Rackspace. With respect to such interaction with a Supervisory Authority, Supplier shall (and shall cause its personnel and Sub-processors to):

(A) make itself readily available for meetings with the Supervisory Authority as reasonably requested;

(B) subject to Section 10.2(C), answer the Supervisory Authority's questions truthfully, fully and promptly; and provide the Supervisory Authority with such information and cooperation as the Supervisory Authority may require; and

(C) where permitted by law, notify Rackspace of any Supervisory Authority's request for information relating to Rackspace or the Rackspace Personal Data and before disclosing such requested information, cooperate with Rackspace's efforts to prevent the disclosure of, or obtain protective treatment for, such information, and comply with Rackspace's reasonable instructions regarding the response to such request. Any confidential information disclosed by Supplier in accordance with this Section 10.2 shall be disclosed subject to the confidentiality obligations of the Agreement.

11. SUPPLIER INDEMNITY. In addition to Supplier's indemnification obligations set forth in the Agreement, Supplier shall also indemnify, hold harmless, and (upon Rackspace's request) defend Rackspace and its respective directors, officers, employees, subcontractors and agents from any suits, claims, damages, demands, proceedings, and other actions brought by a third party, and all associated expenses and costs (including but not limited to: assessments, fines, losses, penalties, costs of investigating and responding to any Security Incident, costs of notifying affected individuals, and attorneys' fees), arising out of or related to Supplier's or its Subprocessor's collection, processing, storage, use, transmission or destruction of Rackspace Personal Data or Rackspace Information, including, but not limited to, a suspected or actual Security Incidents. The remedies set forth herein shall be in addition to any other remedies available to Rackspace at law or in equity, including but not limited to Supplier's general indemnification obligations set forth in the Agreement.

12. GENERAL.

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

12.2. In the event that there are any inconsistencies between this DPA and the Agreement, this DPA shall prevail as it relates to data privacy or data protection. In the event there are any inconsistencies between this DPA and the applicable Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.3. All third party rights are excluded (except those granted to Rackspace Affiliates under Section 2 and to Data Subjects under the Standard Contractual Clauses). For the avoidance of doubt no person who is not a Party to this DPA shall accrue rights

12.4. The Parties agree that Rackspace's Affiliates are intended third party beneficiaries of the privacy and data security provisions of this DPA and such provisions are intended to inure to the benefit of Rackspace's Affiliates. Without limiting the foregoing, Rackspace's Affiliates will be entitled to enforce all privacy and data security provisions of this DPA as if each was a signatory to this DPA.

12.5. Unless otherwise required by Applicable Data Protection Law or otherwise stated in this DPA, the provisions of the governing law section of the Agreement shall apply to the DPA.

EXHIBIT 1

1. Details of Processing (regardless of whether the Standard Contractual Clauses apply or not). As described in Annex/Appendix 1(B) below.

2. For the purpose of the Approved EU SCCs the following provisions shall apply:

2.1. Module Two. Where Supplier is acting as Rackspace's Processor, Module Two of the Approved EU SCCs shall apply.

2.2. Module Three. Where Supplier is acting as Rackspace's sub-processor, Module Three of the Approved EU SCCs shall apply.

2.3. Clause 7 (docking clause) of the Approved EU SCCs shall apply solely for Affiliates.

2.4. Clause 8 (Data protection safeguards) of the Approved EU SCCs shall be construed by reference to:

(A) Section 4.2 and 4.2(B) of this DPA, for the purposes of Section II, Clause 8.1 (Instructions) of the Approved EU SCCs;

(B) Section 4.10 and 6 of this DPA for the purposes of Section II, Clause 8.9 (Documentation and compliance) of the Approved EU SCCs; and

(C) Section 4.9 of this DPA for the purposes of Section II, Clause 8.5 (Duration of processing and erasure and return of data) of the Approved EU SCCs.

2.5. Clause 9, Option 2 (general written authorization for sub-processors) of the Approved EU SCCs shall apply and the Parties agree that the time period for informing the data exporter of any changes to its list of shall be 60 days.

2.6. Clause 17 (governing law) of the Approved EU SCCs: subject to Section 0 of this DPA, 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 Germany.

2.7. Clause 18 (choice of forum and jurisdiction) of the Approved EU SCCs: subject to Section 5.3 of this DPA, notwithstanding anything to the contrary in the Agreement and unless otherwise required by law or the International Data Transfer Addendum, any dispute arising from the Approved EU SCCs shall be subject to the jurisdiction of, and resolved by, the courts of Germany.

3. For the purpose of the Approved EU SCCs the following provisions shall apply as indicated:

3.1. ANNEX/APPENDIX 1 (OF THE APPROVED EU SCCs).

A. List of Parties.

Data Exporter(s)	**Rackspace contracting entity (or an Affiliate on whose behalf the Rackspace contracting entity enters into the Agreement)**
Address	19122 U.S. Highway 281 N. Ste. 128 San Antonio, TX 78258-7667, United States

Contact person	Chief Privacy Officer, privacy@rackspace.com
Activities relevant to the data transferred under the clauses	The receipt of Services from Supplier, as provided for in the Agreement
Signature and date	Rackspace's acceptance and date of acceptance of the Agreement constitutes signature and date herein
Role	Controller or Processor

Data Importer(s)	**Supplier**
Address	The address Supplier designates in Supplier Agreement
Contact person	The individuals designated as contact(s) on Supplier Agreement or account.
Activities relevant to the data transferred under the clauses	Supplier is a Processor or Sub-processor to Rackspace and provides services to support Rackspace's services.
Signature and date	Supplier's acceptance and date of acceptance of an applicable Supplier Agreement or Order constitutes signature and date herein.
Role	Processor or sub-processor

B. Description of Transfer.

Categories of data subjects whose personal data is transferred

Rackspace's prospects, Customers, business partners, and suppliers who are natural persons; employees or contact persons of Rackspace or its Customers; prospects, customers, business partners; employees, agents, advisors, freelancers of Customers; Customer's users authorized by Rackspace to use the Services.

Categories of personal data (including special category personal data) transferred

Personal Data including but not limited to email, documents, and other data in an electronic form as may be transmitted or stored by Rackspace or Customers in the context of the Services. Depending on the type of Services provided by Supplier, the following categories may be included:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;

- Authentication data (for example user name, password or PIN code, security question, audit trail);

- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);

- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);

- Pseudonymous identifiers;

- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);

- Commercial Information (for example history of purchases, special offers, subscription information, payment history);

- Biometric Information (for example DNA, fingerprints and iris scans);

- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of Wi-Fi access points);

- Photos, video and audio;

- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);

- Device identification (for example IMEI-number, SIM card number, MAC address);

- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);

- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);

- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);

- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);

- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;

- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or

- Any other personal data identified in Article 4 of the EU GDPR or UK GDPR.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuously, for the length of the Agreement between the Parties or until otherwise notified by Rackspace.

Subject matter and nature of the processing

Personal Data will be processed for purposes of fulfilling Supplier's obligations to provide goods and/or services to Rackspace (a multicloud technology service provider) or Rackspace's Customers with such obligations to be more specifically described under the applicable Agreement and DPA.

Purpose(s) of the data transfer and further processing

Personal Data will be processed for purposes of fulfilling Supplier's obligations to provide Services to Rackspace (a multicloud technology service provider) or Rackspace's Customers with such obligations to be more specifically described under the applicable Agreement and DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data shall be retained for the length of time necessary to provide the Services under the Agreement or as otherwise required by Applicable Data Protection Law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Supplier's Sub-processors will process Personal Data to assist Supplier in providing the Services pursuant to the Agreement, for as long as needed for Supplier to provide the Services.

C. Competent Supervisory Authority. Unless otherwise required by applicable law, (i) for EEA Personal Data, where Rackspace is established in the EEA, the supervisory authority of the EEA member state in which Rackspace is established; (ii) for EEA Personal Data, where Rackspace is not established in the EEA, the Data Protection Authority of Bavaria for the Private Sector (Bayerisches Landesamt für Datenschutzaufsicht), Promenade 27, 91522 Ansbach, Germany;(iii) for Swiss Personal Data, the Swiss Data Protection Authority; and (iv) where the UK International Data Transfer Addendum applies, the ICO (as defined in the Approved Addendum).

3.2. ANNEX/APPENDIX 2 (OF THE APPROVED EU SCCs).

Technical and Organizational Measures. See Rackspace Secure Information Addendum at www.rackspace.com/information/legal/SSIA, Supplier's obligations in section 4.5 of the DPA and such other security-related obligations as the Parties may have agreed in the Agreement.

4. UK International Data Transfer Addendum

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers (as defined by the Information Commissioner's Office). The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1

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: Rackspace contracting entity (or an Affiliate on	Full legal name: Supplier (as defined in the Agreement).

	whose behalf the Rackspace contracting entity enters into the Agreement). Main address (if a company registered address): 19122 U.S. Highway 281 N. Ste. 128 San Antonio, TX 78258-7667, United States. Official registration number (if any) (company number or similar identifier): The company registration number of Rackspace.	Main address (if a company registered address): The address Supplier designates on Supplier's account. Official registration number (if any) (company number or similar identifier): The official registration number designated in the Supplier's account, if any.
Key Contact	Full Name (optional): Job Title: Chief Privacy Officer Contact details including email: 19122 U.S. Highway 281 N. Ste. 128 San Antonio, TX 78258-7667, United States privacy@rackspace.com	Full Name (optional): Job Title: The job title of the Supplier contact in the Rackspace supplier account system, if any. Contact details including email: The job title of the Supplier contact in the Rackspace supplier account system, if any.

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. Reference (if any): N/A. Other identifier (if any): N/A

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: Section 3 to this Exhibit 1.

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

Ending this Addendum when the Approved Addendum changes	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.

EXHIBIT 2 – Approved KSA Standard Contractual Clauses

For the purposes of these Approved KSA Standard Contractual Clauses:

Clauses 1-12 shall be as provided on the KSA SDAIA website found at https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf or successor URL.

Clause 13: Protection of Transferred Personal Data.

- Second Template. Where Supplier is acting as Rackspace's Processor, the Second Template (Controller to Processor) of the KSA SCCs shall apply.

- Third Template. Where Supplier is acting as Rackspace's sub-processor (Processor to Processor), the Third Template of the KSA SCCs shall apply.

APPENDIX 1- List of Parties

Data Exporter(s) Information:

Name:	Rackspace contracting entity (or an Affiliate on whose behalf the Rackspace contracting entity enters into the Agreement)
Address:	19122 U.S. Highway 281 N. Ste. 128 San Antonio, TX 78258-7667, United States
Point of Contact Information:	Chief Privacy Officer, privacy@rackspace.com
Signature:	Rackspace's acceptance and date of acceptance of the Agreement constitutes signature and date herein
Date:	Rackspace's acceptance and date of acceptance of the Agreement constitutes signature and date herein
Role:	Controller or Processor

Data Importer(s) Information:

Name:	Supplier
Address:	The address Supplier designates in Supplier Agreement
Point of Contact Information:	The individuals designated as contact(s) on Supplier Agreement or account.
Signature:	Supplier's acceptance and date of acceptance of an applicable Supplier Agreement or Order constitutes signature and date herein.
Date:	Supplier's acceptance and date of acceptance of an applicable Supplier Agreement or Order constitutes signature and date herein.
Role:	Processor or sub-processor

APPENDIX 2- Description of the Transferred Personal Data

Categories of data subjects whose personal data is transferred:
Rackspace's prospects, Customers, business partners, and suppliers who are natural persons; employees or contact persons of Rackspace or its Customers; prospects, customers, business partners; employees, agents, advisors, freelancers of Customers; Customer's users authorized by Rackspace to use the Services.

Categories of personal data transferred Personal Data
Personal Data including but not limited to email, documents, and other data in an electronic form as may be transmitted or stored by Rackspace or Customers in the context of the Services. Depending on the type of Services provided by Supplier, the following categories may be included:
• Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
• Authentication data (for example user name, password or PIN code, security question, audit trail);
• Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
• Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
• Pseudonymous identifiers;
• Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
• Commercial Information (for example history of purchases, special offers, subscription information, payment history);
• Biometric Information (for example DNA, fingerprints and iris scans);
• Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of Wi-Fi access points);
• Photos, video and audio;
• Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
• Device identification (for example IMEI-number, SIM card number, MAC address);

• Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
• HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
• Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
• Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
• Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;

Categories of transferred sensitive data- if any -and applicable restrictions and safeguards that take full account of the nature of the Personal Data and the risks involved, eg. Purpose limitation, access, restrictions, record keeping of access to Personal Data, restrictions on subsequent transfers, or additional organizational, technical and regulatory measures:
• Special categories of data (for example racial or ethnic origin, political opinions, intellectual, political, religious and/or philosophical beliefs, trade union membership, genetic data, biometric data (for example DNA, fingerprints and iris scans) for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to security convictions and/or criminal convictions or offences, and data that one or both of the individual's parents are unknown).
• For organizational, technical and regulatory measures see Rackspace Secure Information Addendum at www.rackspace.com/information/legal/SSIA, Supplier's obligations in section 4.5 of the DPA and such other security-related obligations as the Parties may have agreed in the Agreement.

Purpose of Transfer:
Personal Data will be processed for purposes of fulfilling Supplier's obligations to provide Services to Rackspace (a multicloud technology service provider) or Rackspace's Customers with such obligations to be more specifically described under the applicable Agreement and DPA.

Retention Period:
Continuously, for the length of the Agreement between the Parties or until otherwise notified by Rackspace.

APPENDIX 3- Security Measures

See Rackspace Secure Information Addendum at www.rackspace.com/information/legal/SSIA, Supplier's obligations in section 4.5 of the DPA and such other security-related obligations as the Parties may have agreed in the Agreement.