INTRA-COMPANY DATA PROCESSING AGREEMENT

between

Rackspace International GmbH
Pfingstweidstrasse 60, 8005 Zurich, Switzerland

and

Rackspace Limited
5 Millington Road, Hyde Park Hayes, Middlesex, UB3 4AZ, UK

and

Rackspace US, Inc.
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

Rackspace Asia Limited
9/F., Cambridge House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong

and

Rackspace Hosting Australia Pty Limited
Level 1, 37 Pitt Street, Sydney, NSW 2000, Australia

and

Rackspace Germany GmbH
Luise-Ullrich-Strasse 20, 80636 Munich, Germany

and

Rackspace Singapore Pte. Ltd
Chevron House, 30 Raffles Place, 23/F, Singapore 048622, Singapore

and

Rackspace Mexico
Plaza Carso, Lago Zurich 219, Torre II, Piso 11, Colonia Ampliación Granada, Mexico City 11590, Mexico
and

Rackspace Benelux B.V.
Radarweg 535, 1043 NZ Amsterdam, Netherlands

and

TriCore Solutions Private Limited
T-2528, II nd floor, Office no 1A, Gurunanak Market, Faiz Road, Karol Bagh, New Delhi 110005

and

Datapipe, Inc
Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808

and

Datapipe Government Solutions, Inc
Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808

and

Datapipe Europe Ltd.
20-22 Commercial St, London E1 6LP, United Kingdom

and

Datapipe Asia, Ltd.
19/F, Seaview Commercial Building, 21-24 Connaught Road West, Hong Kong

and

Datapipe Asia (Shanghai), Ltd.
Room 3151, 31 Floor, 88 Century Avenue Jinmao Tower, Shanghai free trade zone, China

and

Datapipe Singapore PTE Ltd.
143 Cecil Street, #08-01, GB Building, Singapore 069542
and

RelationEdge, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

RelationEdge Seattle, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

RelationEdge San Diego, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

RelationEdge New York, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

RelationEdge Los Angeles, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

RelationEdge Denver, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

RelationEdge Dallas, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and

RelationEdge Chicago, LLC
1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218, USA

and
Whereas, the Parties provide hosting services and/or ancillary services directly or indirectly to the Parties’ customers;

Whereas, any of the Parties may Process Personal Data in the function of Controller and may transfer this Personal Data to any of the Parties, so that any Party may act as Data Exporter or as Data Importer, as the case may be;

Whereas, the Parties wish to ensure that the transfer of Personal Data from Data Exporter to Data Importer is done in compliance with the requirements of (i) the EU General Data Protection Regulation (EU) 2016/679; (ii) EU-U.S. Privacy Shield when applicable; and (iii) the EU Standard Contractual Clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, when applicable; and

Therefore, the Parties have agreed to include the following provisions that are required by Applicable Data Protection Law (defined below) to be stipulated in the contract with Processors and Sub-processors and other related terms.

1. DEFINED TERMS. For the purposes of this Agreement, the following definitions apply:

“Affiliate” means any legal entity that a Party owns, that owns a Party, or that is under its common ownership. “Ownership” means, for the purposes of this definition, control of more than a fifty percent interest in an entity;

“Agreement” means this agreement between the Parties in relation to the processing of Personal Data;

“Applicable Data Protection Law” means all applicable laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations in relation to data privacy, including but not limited to the EU General Data Protection Regulation ((EU) 2016/679), in each case together with any transposing, implementing or supplemental legislation; and “Personal Data”, “Process/Processing”, “Controller”, “Processor”, and “Data Subjects” shall have the meanings given to them in Applicable Data Protection Law;

“Applicable Rackspace Entity” means any Rackspace Group entity that is established outside the EEA, to the extent that the Controller (i) stores Personal Data in a data center outside the EEA operated by such Rackspace Group entity or (ii) receives services located in the EEA from such Rackspace Group entity;

“Customer” means a customer of any Applicable Rackspace Entity for the provision of the Services;

“Rackspace Group” means Rackspace US, Inc. and its Affiliates.

“Security Incident” means a breach of security by the Processor leading to (i) accidental or unlawful destruction of Personal Data or (ii) loss, alteration, unauthorised disclosure of, or access to Personal Data.

“Services” means the managed hosting and support services and any other related services (including the detection, prevention and resolution of security and technical issues) provided to the relevant Customer.

“Standard Contractual Clauses” means the standard contractual clauses (processors) for the transfer of personal data set out in the EU Commission Decision of 5 February 2010 (2010/87/EC); and
“subprocessor”, “Data Importer”, and “Data Exporter” shall have the meanings given to them in the Standard Contractual Clauses; and

“Transfer Protections” means, in relation to a transfer of Personal Data to countries outside of the EEA (including any such transfers to Applicable Rackspace Entities their subprocessors), measures to enable the transfer to be made in compliance with Applicable Data Protection Law, including without limitation where the recipient of such data: (i) receives such data in a country that the European Commission has decided provides adequate protection for Personal Data (including where the recipient has subscribed to the Privacy Shield under the European Commission's Implementing Decision (EU) 2016/1250); (ii) has achieved Binding Corporate Rules authorization in accordance with Applicable Data Protection Law; (iii) has executed Standard Contractual Clauses adopted or approved by the European Commission (including the Standard Contractual Clauses under this Agreement); or (iv) has in place an alternative mechanism that complies with Applicable Data Protection Law for the transfer of Personal Data outside the European Union.

2. PROCESSING OF PERSONAL DATA.

2.1 Processing of Personal Data. The Parties agree that, in respect to any Processing of Personal Data, the Processor shall:

2.1.2 comply with the obligations that apply to it under Applicable Data Protection Law; and

2.1.3 remain in scope with the subject matter of the Processing; the duration of the Processing (which shall be from the date of this Agreement and shall end on termination of this Agreement); the purpose of the Processing; the type of Personal Data Processed; and the categories of Data Subjects made available to the Applicable Rackspace Entity, including employees, contractors, partners of Rackspace or its clients or any of their end users or Customers who are individuals (as detailed in Appendix 1).

2.2 Processor Responsibilities. Where the Applicable Rackspace Entity is acting as a Processor, it shall:

2.2.1 Process the Personal Data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization (instructions on which are set out in section 2.2.4 below), unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

2.2.2 ensure that all personnel (including staff, agents and subcontractors) who the Processor authorizes to Process Personal Data are subject to a duty of confidentiality (whether contractual or statutory);

2.2.3 maintain and implement technical and organizational measures appropriate (having regard to the state of technological development and cost of implementation) to the risk of, and to seek to protect Personal Data against, any Security Incident. Such measures shall include, as appropriate: (a) the pseudonymization 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 Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. At a minimum, such measures shall include the measures set out in Appendix 2;

2.2.4 not transfer any Personal Data outside of the European Economic Area unless it has taken steps to ensure Transfer Protections, but subject to such Transfer Protections the Controller agrees that Personal Data may be Processed in countries where the Processor or its sub processors maintain facilities or personnel;

2.2.5 provide reasonable and timely assistance to the Controller so that it may respond to any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the processing of Personal Data;

2.2.6 if it becomes aware of a Security Incident, inform the Controller without undue delay and provide reasonable information (to the extent that such information is known or available to it) and cooperation to the Controller so that the Controller can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Laws.
Law. The Processor shall further take such any reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and shall keep the Controller informed of material developments in connection with the Security Incident;

2.2.7 taking into account the nature of the Processing and the information available to it, assist the Controller in ensuring compliance with the Controller's obligations pursuant to the data protection impact assessments and prior consultation under Applicable Data Protection Law. If, however, the Processor 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, it shall inform the Controller and provide reasonable cooperation to the Controller (at the Controller's expense) in connection with any data protection impact assessment that may be required under Applicable Data Protection Law;

2.2.8 enable the Controller to retrieve and/or delete Personal Data in accordance with Applicable Data Protection Law. Where the Controller instructs the Processor to delete all Personal Data in its possession or control, including existing copies thereof, the Processor shall delete such Personal Data but this requirement shall not apply to the extent the Processor is required by applicable law to retain all or some of the Personal Data or to Personal Data it has archived on back-up systems; and

2.2.9 maintain records required by Applicable Data Protection Law and shall make available to the Controller all information necessary to demonstrate its compliance with Applicable Data Protection Law and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

2.3 Subprocessing. The following provisions shall apply in relation to any sub processing:

2.3.1 The Controller authorizes the Processor to engage any Rackspace Group entity, including any Applicable Rackspace Entity, and any third-party subcontractors and/ or resellers (including but not limited to, Amazon, Microsoft, Google and Alibaba) as subprocessors. The Parties agree that the Processor shall (i) maintain and make available to the Controller an up-to-date list of its subprocessors, giving the Controller notice of any change in subprocessors prior to any new subcontractor being authorised to Process any Personal Data by updating the list accordingly; (ii) impose written data protection terms on any subprocessor it appoints that require it to Process any Personal Data only to the extent necessary to provide the services for which it has been engaged by it (and for no other purpose) and to protect the Personal Data to at least the standard required by this Agreement and Applicable Data Protection Law; and (iii) remain liable for any breach of this Agreement that is caused by an act, error or omission of its subprocessor.

2.3.2 For the purposes of (i) Applicable Data Protection Law and (ii) Clause 5(h) and Clause 11 of the Standard Contractual Clauses, the Controller confirms that it has provided its prior written consent to the engagement of the subprocessors.

3. EU DATA TRANSERS. To the extent that EU data transfers occur, the Applicable Rackspace Entity shall comply with the following:

3.1 Privacy Shield. For data transfers directly to the U.S. and any onward transfers, the Applicable Rackspace Entity adheres to both EU-U.S. and U.S.-Swiss Privacy Shield compliance frameworks. Each Rackspace Entity agrees to apply the same or greater level of protection as required by the Privacy Shield Principles (“Principles”) under the relevant Privacy Shield Framework. Details about the requisite Principles under these frameworks can be found at https://www.privacyshield.gov. If the Applicable Rackspace Entity is unable to meet these obligations at any time, then it shall cease all processing of EU or Swiss Personal Data, and adhere to the data transfer, deletion, or destruction protocol as set forth by Rackspace U.S., Inc.

3.2 Standard Contractual Clauses. For EU data transfers directly to countries other than the United States and Switzerland, that have not been recognized by the EU Commission as a country which ensures an adequate level of protection within the meaning of Applicable Data Protection Law, the Applicable Rackspace Entity shall implement EU Standard Contractual Clauses or other legally-valid, EU-approved data transfer mechanism, if applicable, and the Standard Contractual Clauses are incorporated by reference as though fully rewritten herein Exhibit 1.
4. **GENERAL**

4.1 **Governing Law.** This Agreement is governed by and construed in accordance with the law of England and Wales.
Exhibit 1 – Standard Contractual Clauses

Clause 1

Definitions

For the purposes of the Clauses:

(a) “Personal Data”, “Special Categories of Data”, “Process/Processing”, “Controller”, “Processor”, “Data Subject” and “Supervisory Authority” shall have the meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) “the Data Exporter” means the Controller who transfers the Personal Data;

(c) “the Data Importer” means the Processor who agrees to receive from the Data Exporter Personal Data intended for Processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses;

(d) “the Sub-processor” means any Processor engaged by the Data Importer or by any other sub-processor of the Data Importer who agrees to receive from the Data Importer or from any other sub-processor of the Data Importer Personal Data exclusively intended for Processing activities to be carried out on behalf of the Data Importer after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) “The Applicable Data Protection Law” means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data applicable to a data Controller in the state in which the Data Exporter is established;

(f) “Technical and Organisational Security Measures” means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the Special Categories of Personal Data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The Data Subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.

3. The Data Subject can enforce against the Sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter.
Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Sub-processor shall be limited to its own Processing operations under the Clauses.

4. The Parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the Processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the state where the Data Exporter is established) and does not violate the relevant provisions of that state;

(b) that it has instructed and throughout the duration of the Personal Data Processing services will instruct the Data Importer to Process the Personal Data transferred only on the Data Exporters behalf and in accordance with the Applicable Data Protection Law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the Technical and Organisational Security Measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the Applicable Data Protection Law, the Technical and Organisational Security Measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the Technical and Organisational Security Measures;

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

(g) to forward any notification received from the Data Importer or any Sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection Supervisory Authority if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the Data Subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the Technical and Organisational Security Measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the Processing activity is carried out in accordance with Clause 11 by a Sub-processor providing at least the same level of protection for the Personal Data and the rights of Data Subject as the Data Importer under the Clauses; and

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

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:
to Process the Personal Data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

c) that it has implemented the Technical and Organisational Security Measures specified in Appendix 2 before Processing the Personal Data transferred;

d) that it will promptly notify the Data Exporter about:

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

(ii) any accidental or unauthorised access, and

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

e) to deal promptly and properly with all inquiries from the Data Exporter relating to its Processing of the Personal Data subject to the transfer and to abide by the advice of the Supervisory Authority with regard to the Processing of the data transferred;

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

g) to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the Technical and Organisational Security Measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;

(h) that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the Processing services by the Sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any Sub-processor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The Parties agree that any Data Subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any Party or Sub-processor is entitled to receive compensation from the Data Exporter for the damage suffered.

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

The Data Importer may not rely on a breach by a Sub-processor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

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

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

   (b) to refer the dispute to the courts of England or in the state in which the Data Exporter is established.

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

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the Supervisory Authority if it so requests or if such deposit is required under the Applicable Data Protection Law.

2. The Parties agree that the Supervisory Authority has the right to conduct an audit of the Data Importer, and of any Sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the Applicable Data Protection Law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Sub-processor preventing the conduct of an audit of the Data Importer, or any Sub-processor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of England.
Clause 10

Variation of the contract

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

Clause 11

Sub-processing

1. The Data Importer shall not subcontract any of its Processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on the Data Importer under the Clauses. Where the Sub-processor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Sub-processors obligations under such agreement.

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

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of England.

4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection Supervisory Authority.

Clause 12

Obligation after the termination of Personal Data Processing services

1. The Parties agree that on the termination of the provision of data Processing services, the Data Importer and the Sub-processor shall, at the choice of the Data Exporter, return all the Personal Data transferred and the copies thereof to the Data Exporter or shall destroy all the Personal Data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

2. The Data Importer and the Sub-processor warrant that upon request of the Data Exporter and/or of the Supervisory Authority, it will submit its data Processing facilities for an audit of the measures referred to in paragraph 1.
Rackspace International GmbH
Name: Reinhard Waldinger, Director

Rackspace US, Inc.
Name: Christopher Rosas, VP of Global Tax

Rackspace Hosting Australia Pty Limited
Name: Christopher Rosas, Director

Rackspace Singapore Pte. Ltd
Name: Christopher Rosas, Director

Rackspace Benelux B.V.
Name: Christopher Rosas, Director A

Datapipe, Inc.
Name: Christopher Rosas, Director

Rackspace Limited
Name: Christopher Rosas, Director

Rackspace Asia Limited
Name: Christopher Rosas, Assistant Treasurer & Secretary

Rackspace Germany GmbH
Name: Christopher Rosas, Director

Rackspace Mexico
Name: Christopher Rosas, Legal Representative

TriCore Solutions Private Limited
Name: Christopher Rosas, Director

Datapipe Government Solutions, Inc.
Name: Christopher Rosas, Director
Datapipe Europe Ltd.
Name: Christopher Rosas
Director

Datapipe Asia, Ltd.
Name: Michael Bross,
Director

Datapipe Asia (Shanghai), Ltd.
Name: Michael Bross,
Legal Representative

Datapipe Singapore PTE Ltd.
Name: Michael Bross,
Director

RelationEdge, LLC
Name: Christopher Rosas
Treasurer & Secretary

RelationEdge Seattle, LLC
Name: Christopher Rosas
Treasurer & Secretary

RelationEdge San Diego, LLC
Name: Christopher Rosas
Treasurer & Secretary

RelationEdge New York, LLC
Name: Christopher Rosas
Treasurer & Secretary

RelationEdge Los Angeles, LLC
Name: Christopher Rosas
Treasurer & Secretary

RelationEdge Denver, LLC
Name: Christopher Rosas
Treasurer & Secretary

RelationEdge Chicago, LLC
Name: Christopher Rosas
Treasurer & Secretary

RelationEdge Atlanta, LLC
Name: Christopher Rosas
Treasurer & Secretary
RelationEdge Dallas, LLC

Name: Christopher Rosas
Treasurer & Secretary

Main Path, LLC (DBA RelationEdge Digital Agency)

Name: Christopher Rosas
Treasurer & Secretary
APPENDIX 1 TO THE CONTRACTUAL CLAUSES ON DATA PROCESSING

Data exporter
The Data Exporter is (please specify briefly your activities relevant to the transfer):
- a provider of managed hosting and support services and any other related services (including the detection, prevention and resolution of security and technical issues)

Data importer
The Data Importer is (please specify briefly activities relevant to the transfer):
- a provider of managed hosting and support services and any other related services (including the detection, prevention and resolution of security and technical issues)

Data subjects
The Personal Data transferred concern the following categories of Data Subjects (please specify):
- customers and prospects
- employees
- contractors
- partners
- third party service providers
- any end - users
- any individual whose Personal Data is processed for provision of services

Categories of data
The Personal Data transferred concern the following categories of data (please specify):
- data processed for provision and receipt of the services including contact details (name, address, email address and contact number) and payment details.

Special categories of data (if appropriate)
The Personal Data transferred concern the following Special Categories of Data (please specify):
- Not applicable

Processing operations
The Personal Data transferred will be subject to the following basic Processing activities (please specify):
Providing managed hosting and support services and any other related services (including the detection, prevention and resolution of security and technical issues).
APPENDIX 2 TO THE CONTRACTUAL CLAUSES ON DATA PROCESSING

Description of the Technical and Organisational Security Measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Rackspace Global Security & Privacy Practices apply which are available at: