DATA PROCESSING AGREEMENT

by and between

Ziflow Limited

with offices at Alton House, 66 High Street, Northwood HA6 1BL United Kingdom

("Data Controller" or "Subscriber")

and

Zendesk, Inc.,
a U.S. corporation formed under the laws of the State of Delaware
with offices at 989 Market Street, San Francisco, CA 94103
("Data Processor" or "Zendesk")

1. PURPOSE

1.1 Data Controller and Data Processor have entered into a Master Subscription Agreement ("MSA") pursuant to which Data Controller is granted a license to access and use the Service during the Subscription Term. In providing the Service, Data Processor will engage, on behalf of Data Controller, in the Processing of Personal Data submitted to and stored within the Service by Data Controller or third parties with whom Data Controller transacts using the Service. Data Controller acknowledges and agrees that Data Processor may receive, collect and/or Process Personal Data based on Our legitimate interest under Applicable Data Protection Law to provide, secure and improve the Services. The terms of this Data Processing Agreement ("DPA") shall only apply to: (a) subject to Section 9, Data Controllers with an active subscription to the Service(s); and (b) Personal Data within Service Data.

1.2 The Parties are entering into this DPA to ensure that the Processing by Data Processor of Personal Data, within the Service by Data Controller and/or on its behalf, is done in a manner compliant with Applicable Data Protection Law.

1.3 To the extent that any terms of the MSA conflict with the substantive terms of this DPA (as they relate to the protection of Personal Data), the terms of this DPA shall take precedence.

2. OWNERSHIP OF THE SERVICE DATA

2.1 As between the Parties, all Service Data Processed under the terms of this DPA and the MSA shall remain the property of Data Controller. Under no circumstances will Data Processor act, or be deemed to act, as a "controller" (or equivalent concept) of the Service Data under any Applicable Data Protection Law.

3. OBLIGATIONS OF DATA PROCESSOR

3.1 The Parties agree that the subject-matter and duration of Processing performed by Data Processor under this DPA, including the nature and purpose of Processing, the type of Personal Data, and categories of Data Subjects, shall be as described in Exhibit A of this DPA.

3.2 As part of Data Processor providing the Service to Data Controller under the MSA, Data Processor shall comply with the obligations imposed upon it under Article 28-32 of the GDPR and agrees and declares as follows:

(i) to process Personal Data in accordance with Data Controller's documented instructions as set out in the MSA and this DPA, also with regard to transfers of personal data to a third country or an international organisation in accordance with Article 28 (3) (a) of the GDPR, unless required to do otherwise by Union or Member State Law to which the Data Processor is subject, or as otherwise necessary to provide the Service. In any such case, Data Processor shall inform

Data Controller of that legal requirement upon becoming aware of the same (except where prohibited by applicable laws);

(ii) to ensure that all staff and management of any member of the Processor Group are fully aware of their responsibilities to protect Personal Data in accordance with this DPA and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in accordance with Article 28 (3) (b) of the GDPR;

(iii) to implement and maintain appropriate technical and organizational measures to protect Personal Data in accordance with Article 32 of the GDPR against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (a "**Data Security Breach**"), provided that such measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, so as to ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected, including:

(a) data security controls in accordance with ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001 as it pertains to the Zendesk Services that are included within the scope of said Report (as defined in Section 5); and

(b) data security controls achieve prevailing industry standards (including, without limitation, Service Organization Controls No. 2 (SOC2) in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) or such other alternative standards that are substantially equivalent to ISO 27001 as it pertains to the Zendesk Services that are included within the scope of said Report.

(iv) to notify Data Controller in accordance with Article 33 (2) of the GDPR, without undue delay but in any event within forty-eight (48) hours, in the event of a confirmed Data Security Breach affecting Data Controller's Personal Data and to cooperate with Data Controller as necessary to mitigate or remediate the Data Security Breach. Further, Data Processor shall cooperate with Data Controller and take such commercially reasonable steps as are directed by the Data Controller to assist in the investigation, mitigation and remediation of any such Data Security Breach under the Applicable Data Protection Law;

(v) to comply with the requirements of Section 4 (Use of Sub-processors) when engaging a Sub-processor;

(vi) taking into account the nature of the Processing, shall assist Data Controller (including by appropriate technical and organizational measures), insofar as it is commercially reasonable, to fulfil Data Controller's obligation to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law (a "**Data Subject Request**"). In the event that Data Processor receives a Data Subject Request directly from a Data Subject, it shall (unless prohibited by law) direct the Data Subject to the Data Controller in the first instance. However, in the event Data Controller is unable to address the Data Subject Request, taking into account the nature of the Processing and the information available to Data Processor, Data Processor, shall, on Data Controller's request and at Data Controller's reasonable expense (scoped prior to Data Processor's response to the Data Subject Request), address the Data Subject Request, as required under the Applicable Data Protection Law;

(vii) upon request, to provide Data Controller with commercially reasonable information and assistance, taking into account the nature of the Processing and the information available to Data Processor, to help Data Controller to conduct any data protection impact assessment or Supervisor consultation it is required to conduct under Applicable Data Protection Law;

(viii) upon termination of Data Controller's access to and use of the Service, to comply with the requirements of Section 8 of this DPA (Return and Destruction of Personal Data);

(ix) to comply with the requirements of Section 5 of this DPA (Audit) in order to make available to Data Controller information that demonstrates Data Processor's compliance with this DPA; and

(x) to appoint a security officer who will act as a point of contact for Data Controller, and coordinate and control compliance with this DPA, including the measures detailed in Exhibits B-1 and B-2 to this DPA, as applicable.

3.3 Data Processor shall immediately inform Data Controller if, in its opinion, Data Controller's Processing instructions infringe any law or regulation. In such event, Data Processor is entitled to refuse Processing of Personal Data that it believes to be in violation of any law or regulation.

4. USE OF SUB-PROCESSORS

4.1 Data Controller hereby confirms its general written authorisation for Data Processor's use of the Sub-processors listed at https://help.zendesk.com/hc/en-us/articles/229138187-Subprocessors-and-Subcontractors in accordance with Article 28 of the GDPR to assist Data Processor in providing the Service and Processing Personal Data, provided that such Sub-processors:

(i) agree to act only on Data Processor's instructions when Processing the Personal Data (which instructions shall be consistent with Data Controller's Processing instructions to Data Processor); and

(ii) agree to protect the Personal Data to a standard consistent with the requirements of this DPA, including by implementing and maintaining appropriate technical and organizational measures to protect the Personal Data they Process consistent with the Security Standards described in Exhibits B-1 and B-2 to this DPA, as applicable.

4.2 Data Processor shall remain liable to Data Controller for the subcontracted Processing services of any of its Sub-processors under this DPA. Data Processor shall maintain an up-to-date list of the names and locations of all Sub-processors used for the Processing of Personal Data under this DPA at https://help.zendesk.com/hc/en-us/articles/229138187-Subprocessors-and-Subcontractors. Data Processor shall update the list on its Website of any Sub-processor to be appointed at least thirty (30) days prior to the date on which the Sub-processor shall commence processing Personal Data. Data Controller may sign up to receive email notification of any such changes. The details of the sign up process are set forth in the aforementioned URL.

4.3 In the event that Data Controller objects to the Processing of its Personal Data by any newly appointed Sub-processor as described in Section 4.2, it shall inform Data Processor within thirty (30) days following the update of its online policy above. In such event, Data Processor will either (a) instruct the Sub-processor to cease the Processing of Data Controller's Personal Data, in which event this DPA shall continue unaffected, or (b) allow Data Controller to terminate this DPA (and any related services agreement with Data Processor) immediately and provide it with a pro rata reimbursement of any sums paid in advance for Services to be provided but not yet received by Data Controller as of the effective date of termination.

4.4 The Service provides links to integrations with Non-Zendesk Services, including, without limitation, certain Non-Zendesk Services which may be integrated directly into Data Controller's account or instance in the Service. If Data Controller elects to enable, access, or use such Non-Zendesk Services, its access and use of such Non-Zendesk Services is governed solely by the terms and conditions and privacy policies of such Non-Zendesk Services, and Data Processor does not endorse and is not responsible or liable for, and makes no representations as to any aspect of such Non-Zendesk Services, including, without limitation, their content or the manner in which they handle Service Data (including Personal Data) or any interaction between Data Controller and the provider of such Non-Zendesk Services. The providers of Non-Zendesk Services shall not be deemed Sub-processors for any purpose under this DPA.

5. AUDIT

5.1 The Parties acknowledge that, excluding Innovation Services, Data Processor uses external auditors to verify the adequacy of its security measures, including the security of the physical data centres from which Data Processor provides its data processing services. This audit:

(i) will be performed at least annually;

(ii) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001;

(iii) will be performed by independent third party security professionals at Data Processor's selection and expense; and

(iv) will result in the generation of an audit report affirming that Data Processor's data security controls achieve prevailing industry standards (including, without limitation, Service Organization Controls No. 2 (SOC2) in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) or such other alternative standards that are substantially equivalent to ISO 27001 ("**Report**").

5.2 At Data Controller's written request and without charge, Data Processor will provide Data Controller with a confidential summary of the Report ("**Summary Report**") so Data Controller can reasonably verify Data Processor's compliance with the security and audit obligations under this DPA. The Summary Report will constitute Data Processor's Confidential Information under the confidentiality provisions of Data Processor's MSA.

5.3 Data Controller agrees that the audit procedures described in Sections 5.1-5.3 above satisfy any right it may have to conduct an audit or inspection under Article 28 of the GDPR, or under the EU Commission's "Controller-to-Processor Standard Contractual Clauses" (annexed to the EU Commission Decision 2010/87/EU and included as Exhibit C of this DPA), if applicable.

6. INTERNATIONAL DATA EXPORTS

6.1 Data Controller acknowledges that Data Processor and its Sub-processors may maintain data processing operations in countries that are outside of the EEA, United Kingdom, and Switzerland. As such, Data Processor and its Sub-processors may Process Personal Data in non-EEA, non-United Kingdom and non-Swiss countries. This will apply even where Data Controller has agreed with Data Processor to host Personal Data in the EEA in accordance with Zendesk's Regional Data Hosting Policy if such non-EEA Processing is necessary to provide support-related or other services requested by Data Controller. If Personal Data is transferred to a country or territory outside of the EEA, then such transfer will only take place if: (a) the non-EEA country in question ensures an adequate level of data protection; (b) one of the conditions listed in Article 46 GDPR (or its equivalent under any successor legislation) is satisfied; or (c) the Personal Data is transferred on the basis of Zendesk's approved binding corporate rules known as the Zendesk Binding Corporate Rules as set out in Section 6.2 and which establish adequate protection of such personal information and are legally binding on the Zendesk Group. Zendesk will further ensure that the transfer is subject to the standard contractual clauses designed to facilitate transfers of Personal Data from the EEA to all third countries that have been adopted by the European Commission and set out in Section 6.3.

6.2 Binding Corporate Rules

Where Data Processor Processes or permits any Sub-processor within the Processor Group to Process Personal Data outside the EEA or Switzerland, Data Processor shall comply in full with the requirements of Data Processor's Binding Corporate Rules (available at https://d1eipm3vz40hy0.cloudfront.net/pdf/ZENDESK-BCR-Controller-Policy.pdf and https://d1eipm3vz40hy0.cloudfront.net/pdf/ZENDESK%20-%20BCR%20Processor%20Policy.pdf) in order to provide adequate protections for the Personal Data that it Processes on behalf of Data Controller.

6.3 Standard Contractual Clauses

Where Data Processor Processes or permits any Sub-processing entity outside the Processor Group to Process Personal Data in non-EEA countries, Data Processor shall comply with the EU Commission's "Controller-to-Processor Model Clauses" (annexed to EU Commission Decision 2010/87/EU) (the "**Clauses**") subject to the following provisions:

(i) When used below, the terms "data exporter" and "data importer" shall have the meaning given to them in the Clauses.

(ii) Audit of Technical and Organisational Measures. The Parties agree that the audits described in Clauses 5(f) and 12(2) shall be conducted in accordance with the provisions of Section 5 of this DPA.

(iii) Sub-processors.
Data exporter provides a general consent to data importer, pursuant to Clause 11, to engage onward sub-processors. Such consent is conditional on data importer's compliance with the sub-processing conditions set forth in Section 4 of this DPA. In accordance with the provisions of Clause 5(h), data exporter agrees that new Sub-processors may be

appointed by data importer in accordance with the provision of Section 4.2 of this DPA and acknowledges and accepts that data exporter has the objection rights documented in Section 4.3 of the DPA.

(iv) Obligation of data importer to provide any onward Sub-processor Agreement in accordance with Clause 5(j) to data exporter.

The Parties agree that upon the request of data exporter, data importer shall provide all relevant information evidencing compliance with Clause 5(j). Should the information provided by data importer be insufficient to demonstrate data importer's compliance with Clause 5(j) then data importer may provide a version of the onward sub-processor agreement with commercially sensitive and/or confidential information removed. Any such information shall be considered Confidential Information under the confidentiality provisions of the data importer's MSA.

(v) Liability. Pursuant to the provisions of Clause 6, any claims brought under the Clauses shall be subject to the terms and conditions set forth in the MSA. In no event shall any party limit its liability with respect to any Data Subject rights under these Clauses.

Nothing in the interpretations in this Section 6.3 is intended to vary or modify the Clauses or conflict with either Party's rights or responsibilities under the Clauses and, in the event of any conflict between the interpretations herein and the Clauses, the Clauses shall prevail to the extent of such conflict.

6.4 To the extent any export from or processing of Personal Data outside the United Kingdom is subject to Applicable Data Protection Law in the United Kingdom ("UK Data Protection Laws"), (i) general and specific references in the Clauses to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 shall be deemed to have the same meaning as the equivalent reference in the UK Data Protection Laws; (ii) references in the Clauses to "the law of the Member State in which the data exporter is established" shall be deemed to mean "the law of the United Kingdom"; and (iii) any other obligation in the Clauses determined by the Member State in which the data exporter is established shall be deemed to refer to an obligation under UK Data Protection Laws.

6.5 Data Processor continues to participate in and comply with the commitments to which it has certified under the EU-U.S. and Swiss-U.S Privacy Shield Frameworks; however, Data Processor does not currently rely on these frameworks as a basis for transfer of Personal Data.

7. OBLIGATIONS OF DATA CONTROLLER

7.1 As part of Data Controller receiving the Service under the MSA, Data Controller agrees to abide by its obligations under Applicable Data Protection Law.

8. RETURN AND DESTRUCTION OF PERSONAL DATA

8.1 Upon the termination of Data Controller's access to and use of the Service, Data Processor will, up to thirty (30) days following such termination at the choice of the Data Controller either (a) permit Data Controller to export its Service Data, at its expense; or (b) delete all Service Data in accordance with the capabilities of the Service in accordance with Article 28 (3) (g) of the GDPR. Following such period, Data Processor shall delete all Service Data stored or Processed by Data Processor on behalf of Data Controller in accordance with Data Processor's deletion policies and procedures. Data Controller expressly consents to such deletion.

9. DURATION

9.1 This DPA will remain in force as long as Data Processor Processes Personal Data on behalf of Data Controller under the MSA.

10. LIMITATION ON LIABILITY

10.1 This DPA shall be subject to the limitations of liability agreed between the Parties set forth in the MSA (and any reference to the liability of a Party means that Party and its Affiliates in the aggregate). For the avoidance of doubt, Data Controller acknowledges and agrees that Data Processor's total liability for all claims from Data Controller or its Affiliates arising out of or related to the MSA and this Agreement shall apply in aggregate for all claims under both the MSA and this DPA.

10.2 For the avoidance of doubt, this section shall not be construed as limiting the liability of either Party with respect to claims brought by Data Subjects.

11. MISCELLANEOUS

11.1 This DPA may not be amended or modified except in writing and signed by both Parties. This DPA may be executed in counterparts. The terms and conditions of this DPA are confidential and each Party agrees and represents, on behalf of itself, its employees and agents to whom it is permitted to disclose such information that it will not disclose such information to any third party; provided, that each Party shall have the right to disclose such information to its officers, directors, employees, auditors, attorneys and third party contractors who are under an obligation to maintain the confidentiality thereof and may disclose such information as necessary to comply with an order or subpoena of any administrative agency or a court of competent jurisdiction, or as reasonably necessary to comply with any applicable law or regulation. Each Party's rights and obligations concerning assignment and delegation under this DPA shall be as described in the MSA. Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns. This DPA and the MSA constitute the entire understanding between the Parties with respect to the subject matter herein, and shall supersede any other arrangements, negotiations or discussions between the Parties relating to that subject-matter.

12. GOVERNING LAW AND JURISDICTION

12.1 This DPA is governed by the laws of Ireland, and is subject to the exclusive jurisdiction of the courts of Dublin. Notices under this DPA shall be sent in accordance with the notice provisions of the MSA.

13. DEFINITIONS

Unless defined in the MSA or the Reseller Subscription Services Agreement, as applicable, all capitalized terms used in this DPA shall have the meanings given to them below:

13.1 Applicable Data Protection Law: means, in addition to the regulations applicable to certain jurisdictions referred to in the Region-Specific Terms set out in the MSA, the following data protection law(s): (i) the EU Regulation 2016/679 entitled "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" ("**GDPR**") and any applicable national laws made under it; (ii) the Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded); and (iii) the Data Protection Act 2018 (c. 12) of the United Kingdom.

13.2 Data Controller: means the first party named above. However, in the event Data Processor is required to process Personal Data on the request of an Affiliate of Data Controller, such Affiliate shall also be deemed as the "Data Controller". Any reference to the Data Controller within this DPA, unless otherwise specified, shall include Data Controller and its Affiliates.

13.3 Data Processor: has the meaning given in Applicable Data Protection Law (and, for the purposes of this DPA, means Zendesk, Inc.).

13.4 Data Subject: means an identified or identifiable natural person who is the subject of Personal Data.

13.5 Master Subscription Agreement: means the agreement between Data Controller and Data Processor for the provision of, and access to, the Service(s).

13.6 Party: means either Data Controller or Data Processor, and "**Parties**" means Data Controller and Data Processor.

13.7 Personal Data: means any information relating to an identified or identifiable natural person, where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

13.8 Processing: means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

13.9 Reseller Subscription Services Agreement: means the subscription services agreement applicable to customers of Zendesk resellers. However, for the purpose of this DPA, any reference to the Master Subscription Services Agreement should be considered a reference to the Reseller Subscription Services Agreement for customers of Zendesk resellers.

13.10 Processor Group: means Data Processor and any entity which controls, is controlled by, or is under common control with, Data Processor.

13.11 Service Data: means a subset of Confidential Information comprised of electronic data, text, messages, communications or other materials submitted to and stored within the Service by Data Controller, its Agents and End-Users in connection with Data Controller's use of such Service, including, without limitation, Personal Data.

13.12 Sub-processor: means any third party data processor engaged by Data Processor, including entities from the Processor Group, who receives Personal Data from Data Processor for processing on behalf of Data Controller and in accordance with Data Controller's instructions (as communicated by Data Processor) and the terms of its written subcontract.

13.13 Supervisor: means any data protection supervisory authority as defined in the GDPR with competence over Data Controller and Data Processor's Processing of Personal Data.

13.14 Website: means the webpage available at: https://www.zendesk.com/company/agreements-and-terms/.

13.15 Zendesk's Regional Data Hosting Policy: means the policy located at https://support.zendesk.com/hc/en-us/articles/360022185194-Regional-Data-Hosting-Policy.

IN WITNESS WHEREOF, the Parties hereto have executed this DPA by their duly authorized officers or representatives as of the last date of execution below ("Effective Date"):

DATA CONTROLLER: Ziflow Limited		**ZENDESK, INC.**	
BY	DocuSigned by: Mat Atkinson 25146C017037430...	**BY**	DocuSigned by: Jason Robman 23B426850904488...
NAME	Mat Atkinson	**NAME**	Jason Robman
TITLE	CXO	**TITLE**	Associate General Counsel
DATE	7/13/2021	**DATE**	7/13/2021

APPROVED BY ZENDESK LEGAL

EXHIBIT A TO DPA
Processing, Personal Data and Data Subjects

1. Data Processor / Data Importer (where applicable):

The Data Processor / Data Importer (where applicable) operates a cloud-based customer services platform, including an online helpdesk ticketing service, cloud-based customer support live chat platform, self-service options and customer-support features. Further information can be found online at www.zendesk.com.

2. Data Controller / Data Exporter:

The Data Controller /Data Exporter (where applicable) is (please specify briefly your activities relevant to the transfer):

Export of limited personal data relating to the use of the Ziflow application.

3. Duration of Processing:

The processing of Personal Data shall endure for the duration of the Subscription Term in the MSA and this DPA.

4. Data Subjects:

Data Controller / Data Exporter (where applicable) may, at its sole discretion, submit Personal Data to the Service(s), which may include, but is not limited to, the following categories of Data Subjects: employees, relatives of employees, customers, prospective customers, service providers, business partners, vendors, advisors (all of whom are natural persons) of Data Controller / Data Exporter and any natural person(s) authorized by Data Controller / Data Exporter to use the Services.

5. Categories of Personal Data:

Data Controller / Data Exporter (where applicable) may, at its sole discretion, submit Personal Data to the Service(s) which may include, but is not limited to, the following categories of data: first and last name, email address, telephone number, address (business or personal), date of birth, communications (telephone recordings, voicemail), customer service information, title.

6. Special Categories of Data (if appropriate):

None

7. Processing Operations:

The subject matter of the processing of the personal data:

The Data Processor / Data Importer (where applicable) will host and process personal data in the course of providing its cloud-based customer services, helpdesk platform services, and its cloud-based customer support live chat platform services to Data Controller / Data Exporter (where applicable).

8. Contact Details:

For Subscriber Personal Data queries arising from or in connection with this DPA, the Parties shall contact the following:

Data Controller / Data Exporter (where applicable)	**Data Processor / Data Importer (where applicable)**
privacy@ziflow.com	privacy@zendesk.com

zendesk

EXHIBIT B-1 TO DPA
Security Standards for Enterprise Services

As of the Effective Date of this DPA, Our Sub-processors, when Processing Personal Data on behalf of Data Controller in connection with the Enterprise Services, shall implement and maintain the following technical and organizational security measures for the Processing of such Personal Data ("Enterprise Services Security Standards"):

1. Physical Access Controls: Our Sub-processors shall take reasonable measures, such as security personnel and secured buildings, to prevent unauthorized persons from gaining physical access to Personal Data, or ensure third parties operating data centers on its behalf are adhering to such controls.

2. System Access Controls: Data Processor shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

3. Data Access Controls: Data Processor shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.

4. Transmission Controls: Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed; and, any transfer of Personal Data to a third-party service provider is made via a secure transmission.

6. Data Protection: Reasonable measures are taken to ensure that Personal Data is protected against accidental destruction or loss.

7. Logical Separation: Data from different Data Processor's subscriber environments is logically segregated on systems managed by the Data Processor to ensure that Personal Data that is collected by different data controllers is segregated from one another.

zendesk

EXHIBIT B-2 TO DPA
Security Standards for Innovation Services

As of the Effective Date of this DPA, Data Processor, when Processing Personal Data on behalf of Data Controller in connection with the Innovation Services, shall implement and maintain the following technical and organizational security measures for the Processing of such Personal Data ("Innovation Services Security Standards"):

1. Physical Access Controls: Data Processor shall take reasonable measures to prevent physical access to prevent unauthorized persons from gaining access to Personal Data.

2. System Access Controls: Data Processor shall take reasonable measures to prevent Personal Data from being used without authorization.

3. Data Access Controls: Data Processor shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff.

4. Transmission Controls: Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom Personal Data has been entered into data processing systems, modified or removed; and, any transfer of Personal Data to a third-party service provider is made via a secure transmission.

6. Logical Separation: Data from different Data Processor's subscriber environments is logically segregated on systems managed by the Data Processor to ensure that Personal Data that is collected by different data controllers is segregated from one another.

zendesk

EXHIBIT C TO DPA

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization: Ziflow Limited

Address: Alton House, 66 High Street,
Northwood HA6 1BL United Kingdom

Tel.: ; fax: ; e-mail:

Other information needed to identify the organization

……

(the data **exporter**)

And

Name of the data importing organization:

Zendesk, Inc.

Address: **989 Market Street, 6th Floor, San Francisco, California- 94103, USA**

Tel.: + **1-888-670-4887**; fax:+**1 415-644-5778**; e-mail: **privacy@zendesk.com**

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1 below.

1. Definitions

For the purposes of the Clauses:

'personal data', **'special categories of data'**, **'process/processing'**, **'controller'**, **'processor'**, **'data subject'** and **'supervisory authority'** shall have the same 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;

'the data exporter' means the controller who transfers the personal data;

'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 and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'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 exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'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 Member State in which the data exporter is established;

'technical and organizational 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.

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.

3. Third-party beneficiary clause

3.1 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.

3.2 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.

3.3 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 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.

3.4 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.

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 Member 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 exporter's 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 organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the 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 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 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).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) 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 contract 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 organizational 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 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.

6. Liability

6.1 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.

6.2 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 or by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.4 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.

7. Mediation and jurisdiction

7.1 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 in the Member State in which the data exporter is established.

7.2 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.

8. Cooperation with supervisory authorities

8.1 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.

8.2 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.

8.3 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).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

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 Clause.

11. Sub-processing

11.1 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-processor's obligations under such agreement.

11.2 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.

11.3 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 the Member State in which the data exporter is established.

11.4 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.

12. Obligation after the termination of personal data processing services

12.1 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.

12.2 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.

On behalf of the data exporter:

Name (written out in full): Mat Atkinson

Position: CXO

Address: Alton House, 66 High Street,
Northwood HA6 1BL United Kingdom

Other information necessary in order for the contract to be binding (if any):

Signature…… DocuSigned by: Mat Atkinson 25146C01703F430... ……

(stamp of organization)

On behalf of the data importer:

Name (written out in full): Jason Robman

Position: Associate General Counsel

Address: 989 Market Street, San Francisco, California 94103 U.S.A.

Other information necessary in order for the contract to be binding (if any):

Signature…… DocuSigned by: Jason Robman 23B426850904488... ……

APPROVED BY ZENDESK LEGAL

(stamp of organization)

Appendix 1 to Exhibit C: the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

Exhibit A of the DPA shall apply.

Data exporter

The data exporter is (please specify briefly activities relevant to the transfer):

Exhibit A of the DPA shall apply.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Exhibit A of the DPA shall apply.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Exhibit A of the DPA shall apply.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Exhibit A of the DPA shall apply.

Processing operations

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

Exhibit A of the DPA shall apply.

Appendix 2 to Exhibit C: the Standard Contractual Clauses

Data importer (and any sub-processor to data importer) shall implement the technical and organizational measures described in Exhibits B-1 and B-2 to the Data Processing Agreement executed between data exporter and data importer.

This Appendix forms part of the Clauses and must be completed and signed by the parties.

DATA EXPORTER

Name: Mat Atkinson

Title: CXO

Authorised Signature DocuSigned by: Mat Atkinson 25146C01703F430...

DATA IMPORTER

Name: Jason Robman

Title: Associate General Counsel

Authorised Signature DocuSigned by: Jason Robman 23B426850904488... APPROVED BY ZENDESK LEGAL