Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the Agreement(s) and is entered by and between the Customer and the Service Provider on the Effective Date. For the avoidance of doubt, this DPA is not valid or legally binding if there is no Agreement(s) in place between the Customer and the Service Provider.

This DPA becomes effective on the 25th May 2018 or on the acceptance of the Agreement(s), whichever is later (the "**Effective Date**").

1. DEFINITIONS

1.1 **Agreement(s)"** means the agreement entered into between Customer and Service Provider for the provision of Service Provider's Services to the Customer.

1.2 **"Customer"** means the customer as defined in the Agreement(s), including all affiliates of that entity, if any.

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

1.4 **"EU Rules"** means the laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, applicable to the processing of Personal Data under the Agreement(s), including (where applicable) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 also known as the General Data Protection Regulation ("**GDPR**").

1.5 **"Privacy Shield**" means the EU-US framework of privacy principles agreed on February 2, 2016 and formally adopted by the European Commission implementing decision C(2016) 4176 final of July 12, 2016, or any other framework for transferring Personal Data from the EEA or Switzerland to the United States that is approved by the European Commission as providing an adequate level of protection pursuant to the EU Rules.

1.6 **"Services"** means the services and other activities to be supplied to or carried out by or on behalf of Service Provider for the Customer pursuant to the Agreement(s).

1.7 "**Service Provider"** means the legal entity which is a party to the Agreement(s) and Processes Personal Data on behalf of the Customer.

1.7 **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of Personal Data from a Data Controller in the EEA to Processors established in third countries under the EU Data Protection Directive 95/46/EC (the "Directive"), or any legislation replacing the Directive, in the form set out in the Annex of European Commission Decision 2010/87/EU (or any alternative or successor Decision that approves new standard contractual clauses for transfers to data processors in third countries), as amended by incorporating the description of the Personal Data to be transferred set out in Appendix 1 to this DPA and the technical and organisational measures to be implemented as set out in Appendix 2 to this DPA. The Standard Contractual Clauses are available on the European Commission's website at the following link: http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc.

2. APPLICABILITY; ROLES OF THE PARTIES

2.1 This DPA amends and supplements the Agreement(s) between the parties. The terms of this DPA will

apply to all processing of Personal Data in relation to the Services provided under the terms of the Agreement(s). This DPA will not apply to the processing of Personal Data, where such processing is not regulated by the EU Rules.

2.2 Capitalized terms used but not defined in this DPA have the meanings assigned to them in the Agreement(s) or the EU Rules. **"Personal Data**" as used in this DPA includes all data relating to Data Subjects located in the EEA and Switzerland that is processed by Service Provider on behalf of the Customer within the scope of the Agreement(s).

2.3 In the context of this DPA, the Customer acts as a Data Controller and the Service Provider acts as a Data Processor with regard to the Processing of Personal Data.

2.4 Service Provider shall carry out the Services and Process the Personal Data received from the Customer as set out in the Agreement(s) or as otherwise notified in writing by the Customer to Service Provider during the term of the Agreement(s). In the event that in Service Provider's opinion a Processing instruction given by the Customer may infringe EU Rules, Service Provider shall immediately inform the Customer upon becoming aware of such a Processing instruction.

2.5 Service Provider shall undertake at all times to comply with the EU Rules and not to perform its obligations under the Agreement(s) in such way as to cause the Customer to breach any of its applicable obligations under the EU Rules and any existing regulations issued by the relevant data protection authorities.

3. DATA PROTECTION

3.1 All Personal Data provided to Service Provider by the Customer or obtained by Service Provider in the course of its work with the Customer should be protected and may not be copied, disclosed or processed in any way without the written authority of the Customer. To the extent that the provisions of the Agreement(s) or the instructions of the Customer necessitate the copying, disclosure or processing of data, this will be deemed to constitute the required authority to do so.

3.2 Service Provider agrees to comply from time to time with any reasonable measures required by the Customer to ensure its obligations under this DPA are satisfactorily performed in accordance with all applicable legislation. This includes any best practice guidance the Customer notifies Service Provider of.

4. PROCESSING PERSONAL DATA

4.1 Where Service Provider processes Personal Data (whether stored in the form of physical or electronic records) on behalf of the Customer it shall:

4.1.1 Process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations under the Agreement(s) or as is required by law including the EU Rules and any existing laws, rules or regulations issued by the relevant data protection authorities;

4.1.2 Implement appropriate technical and organisational measures and take the steps necessary to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested by the Customer; such security measures are set out in Section 6 of this DPA; and

4.1.3 At the Customer's request, promptly supply the Customer with details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access.

4.2 Customer acknowledges and agrees that (a) Service Provider's affiliates may be retained as Sub-processors; and (b) Service Provider and Service Provider's affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Service Provider will ensure that any third party to which it sub-contracts any processing has entered into a written contract with Service Provider containing similar provisions to those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. Upon Customer's request, Service Provider shall make available to Customer the current list of sub-processors with their country of location. If Service Provider provides hosting services under the Agreement(s), the Customer agrees and acknowledges that Service Provider is allowed to host the Personal Data at a third-party data center provider.

4.3 Unless applicable laws require retention of such Personal Data, Service Provider agrees that in the event that it is notified by the Customer that it is not required to provide any further services to the Customer under this DPA, Service Provider shall transfer a copy of all information (including Personal Data) held by it in relation to this DPA to the Customer in a format chosen by the Customer (provided that the Customer pays for the associated costs) and/or, at the Customer's request, destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the Customer with a written confirmation of secure disposal.

4.4 All copyright, database right and other intellectual property rights in any Personal Data processed under this DPA (including but not limited to any updates, amendments or adaptations to the Personal Data by either the Customer or Service Provider) will belong to the Customer. Service Provider is licensed to use such data only for the term of and in accordance with this DPA.

5. RIGHTS OF DATA SUBJECTS

5.1 Service Provider shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making (each a "**Data Subject Request**"). Taking into account the nature of the Processing, Service Provider shall assist Customer by appropriate technical and organizational measures, to the extent possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Chapter III of the GDPR. Except to the extent required by applicable law, Service Provider shall not respond to any such Data Subject Request without Customer's prior written consent except to confirm that the request relates to Customer.

5.2 Further, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Service Provider shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Service Provider is legally permitted to do so and provided that such Data Subject Request is required under applicable EU Rules. Any costs arising from such provision of assistance shall be the responsibility of Customer, to the extent legally permitted.

6. SECURITY

6.1 Taking 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, Service Provider shall ensure that in respect of all Personal Data it receives from or processes on behalf of the Customer it shall maintain security measures to a standard appropriate to the: (a) harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the Personal Data; and (b) nature of the Personal Data.

6.2 Service Provider shall, with regard to Personal Data, implement and maintain appropriate technical and organizational security measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, and particularly those related to possible Personal Data Breaches. Specifically, Service Provider shall:

6.2.1 have in place and comply with a security policy which: (a) defines security needs based on a regular Privacy Impact Assessment ("PIA"); (b) allocates responsibility for implementing the policy to a specific individual or members of a team, including having a Data Protection Officer ("DPO") in place; (c) 5.3.1.3 is disseminated to all relevant members, volunteers and staff; and (d) provides a mechanism for feedback and review;

6.2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

6.2.3 prevent unauthorised access to the Personal Data;

6.2.4 ensure its storage of Personal Data conforms with the industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

6.2.5 have secure methods in place for the transit of Personal Data within the customer support portal (for instance, by using encryption);

6.2.6 use password protection on computer systems on which Personal Data is stored and ensure that only authorised personnel are given details of the password;

6.2.7 take reasonable steps to ensure the reliability of any employee, agent, contractor or other individuals who have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Agreement(s), and to comply with EU Rules in the context of that individual's duties to the Service Provider;

6.2.8 ensure that any employees, agents, contractors or other individuals required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this DPA;

6.2.9 ensure that none of the employees, agents, contractors or other individuals who have access to the Personal Data publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Customer;

6.2.10 have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of Personal Data) including: (a) the ability to identify which individuals have worked with specific Personal Data; and (b) having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the EU Rules, including written records.

6.2.11 have a secure procedure for backing up and storing back-ups separately from originals; and

6.2.12 have a secure method of disposal for unwanted Personal Data including back-ups, disks, print outs and redundant equipment.

6.3 Service Provider shall provide the Customer with relevant documentation, such as an audit report (upon a written request and subject to obligations of confidentiality), with regard to any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, when the Customer reasonably considers that such data protection impact assessments or prior consultations are required pursuant to Article 35 or 36 of the GDPR or pursuant to the equivalent provisions of any other EU Rule, but in each such case solely with regard to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Service Provider. Such audit will be conducted at the Customer's cost and expense, to the extent legally permitted.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 Service Provider shall, in accordance with the EU Rules, notify the Customer and/or the supervisory authority as soon as any (the "Personal Data Breach") with respect to the Personal Data occurs, but no later than 48 hours from the discovery of such a Personal Data Breach. Service Provider's notification of or response to a Personal Data Breach under this Section 7.1 will not be construed as an acknowledgement by Service Provider of any fault or liability with respect to the Personal Data Breach.

7.2 Service Provider will use reasonable efforts to identity the cause of such Personal Data Breach and shall promptly and without undue delay: (a) investigate the Personal Data Breach and provide Customer with information about the Personal Data Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Article 33(3) of the GDPR to the extent such information is reasonably available ; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach to the extent the remediation is within Service Provider's reasonable control The obligations herein shall not apply to any breach that is caused by Customer or authorized users. Notification will be delivered to Customer in accordance with Section 7.3 below.

7.3 Notification(s) of Personal Data Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Service Provider selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on Service Provider's support systems at all times.

8. OBLIGATIONS OF THE CUSTOMER

The Customer is solely responsible for:

8.1 Complying, at all times with the EU Rules with respect to the processing of Personal Data in connection with the Agreement(s) and the Services;

8.2 Ensuring the processing of the Personal Data by Service Provider is lawful;

8.3 Where applicable, ensuring that legally binding consents to the collection, access, use, maintenance, and/or disclosure of the Personal Data in accordance with the EU Rules and Customer policies and procedures have been obtained from each individual and entity (including without limitation consumers, business customers, and/or Customer employees and contractors) to whom the Personal Data relates;

8.4 Rendering any Personal Data on its systems unusable, unreadable, or indecipherable to unauthorized individuals in accordance with industry standards, applicable law, and any relevant Codes of Conduct;

8.5 Establishing the applicable information security safeguards and associated policies for protecting Personal Data in its facilities. Customer must communicate the relevant safeguards and policies to Service Provider with reasonable advance notice and in writing when Service Provider provides Services at a Customer facility or accesses Customer's systems;

8.6 Promptly informing Service Provider of any policies it implements with respect to the processing and protection of Personal Data with express instructions as to how these policies should be implemented by Service Provider;

8.7 Promptly informing Service Provider of any request for erasure with respect to Data Subject's Personal Data with detailed instructions as to how Service Provider should address the request; and

8.8 Providing to Service Provider and also promptly update, when necessary, the information indicated below (where applicable): (a) identity and contact information of the Data Protection Officer of the Customer; (b) identity and contact information of the EU representative of the Customer; (b) description of the categories of Processing carried out by Customer with respect to the Services; (c) types of Personal Data to be Processed; and (d) categories of Data Subjects to whom the Personal Data relates.

9. INTERNATIONAL DATA TRANSFERS

9.1 Service Provider will only transfer Personal data outside the EEA, where such transfers are regulated by the EU Rules, in compliance with the EU Rules. The Customer authorizes Service Provider (and authorizes Service Provider to authorize its Sub-processors) to Process Personal Data and to transfer Personal Data to those countries or territories where those Sub-processors are located, consistent with the Agreement(s) and this DPA.

9.2 **Transfers Pursuant to the Standard Contractual Clauses**

9.2.1 The Standard Contractual Clauses shall apply to Personal Data that is transferred from the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive and any successor legislation thereto), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to the EU-U.S. Privacy Shield Framework.

9.2.2 Where the Standard Contractual Clauses apply in accordance with Section 9.2.1:

9.2.2.1 Service Provider agrees to comply with the terms of the Standard Contractual Clauses, for the purposes of which Customer and those of its affiliates established in the EEA will be regarded as the Data Exporter(s) and Service Provider will be regarded as the Data Importer;

9.2.2.2 the governing law in clause 9 of the Standard Contractual Clauses shall be the law of the Data Exporter;

9.2.2.3 if so required by the laws or regulatory procedures of any jurisdiction, the parties or Service Provider and any one or more of its affiliates established in the EEA as required, shall execute or re-execute the Standard Contractual Clauses as separate documents setting out the proposed transfers of Personal Data in such manner as may be required;

9.2.2.4 in the event of inconsistencies between the provisions of the Standard Contractual Clauses and this DPA, the Agreement or other agreements between the parties as regards the Services, the Standard Contractual Clauses shall take precedence;

9.2.2.5 in the event that the Standard Contractual Clauses are amended, replaced or repealed by the European Commission or under EU Rules, the parties shall work together in good faith to enter into any updated version of the Standard Contractual Clauses or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with EU Rules; and

9.2.2.6 the parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request.

9.3 **Transfers Pursuant to the Privacy Shield**

9.3.1 In relation to Personal Data which is transferred by Customer to Vendor pursuant to the EU-U.S. or Switzerland-U.S. Privacy Shield Framework, Vendor shall only process such Personal Data strictly in accordance with the E.U.-U.S. or Switzerland-U.S. Privacy Shield Principles and Supplemental Principles.

10. GENERAL TERMS

10.1 Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section of the Agreement(s), and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Agreement(s) and this DPA.

10.2 No alteration, amendment, or modification of this DPA will be valid unless in writing and signed by an authorized representative of both parties.

10.3 Any ambiguity in the terms of this DPA will be resolved to permit Service Provider or Customer to comply with applicable laws.

10.4 This DPA is the entire and complete agreement between the parties with respect to the privacy and security of Personal Data and supersedes any other agreements, representations, or understandings whether oral or written. All clauses of the Agreement(s), that are not explicitly amended or supplemented by the clauses of this DPA, and as long as this does not contradict with compulsory requirements of EU Rules, under this DPA, remain in full force and effect and shall apply, including, but not limited to: Governing Law and Dispute Resolution, Jurisdiction, Limitation of Liability (to the maximum extent permitted by the EU Rules).

10.5 Should any provision of this DPA be found invalid or unenforceable pursuant to any applicable law, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the DPA will continue in effect.

10.6 If Service Provider makes a determination that it can no longer meet its obligations in accordance with this DPA, it shall promptly notify the Customer of that determination, and cease the Processing or take other reasonable and appropriate steps to remediate.

10.7 Notices required under this DPA shall be to be sent according to the Agreement(s) with a copy (which shall not constitute notice via e-mail to: privacy@kayako.com.

10.8 This DPA may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

EXECUTED by and on behalf of:

KAYAKO LIMITED
("Service Provider")

Andrew S Price
Andrew S Price (May 26, 2018)

Signature

Andrew S. Price

Print Name

Chief Financial Officer

Title

May 26, 2018

Date

EXECUTED by and on behalf of:

("Customer")

Signature

Print Name

Title

Date

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual 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 Exporter

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

Data Exporter is the legal entity that has executed the Agreement(s) with the Data Importer.

Data Importer

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

The Data Importer is the legal entity that has executed the Agreement(s) with the Data Exporter, which processes Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement(s).

Data Subjects

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

Categories of Data Subjects, as determined by the Data Exporter, may include customer representatives and (end) users, such as employees, job applicants, contractors, collaborators, partners, suppliers and customers of the Customer.

Categories of data

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

Categories of Personal Data, as determined by the Data Exporter, may include, among other information, personal contact information such as name, address, telephone or mobile number, fax number, email address, and passwords; employment details including employer name, job title and function, and business contact details.

Special categories of data (if appropriate):

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

None.

Purposes of the transfer / Processing operations

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

The objective of Processing of Personal Data by Data Importer is the performance of the Services pursuant to the Agreement(s) in place between the Data Exporter and the Data Importer.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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):

The Data Importer will implement reasonable administrative, physical, managerial and technical controls safeguards for protection of the security, confidentiality and integrity of Personal Data with respect to the Services in accordance with applicable legal requirements, and as set forth in Data Importer's Section 6 of this DPA, and as otherwise agreed by the parties in writing. Data Importer will not materially decrease the overall security of the Services during the term of the Agreement(s).