Mattermost, Inc.
Data Processing Addendum

This Data Processing Addendum ("DPA") in an addendum to the Cloud Subscription License Agreement between Mattermost, Inc. ("Data Processor" or "Mattermost") and the other party entering into the Cloud Subscription License Agreement with Mattermost ("Data Controller"),and describes how Mattermost Processes Personal Data in compliance with Applicable Data Protection Law. The terms of this DPA shall only apply to Data Controllers with an active subscription to Mattermost products or service (collectively, the "Service") under a Cloud Subscription License Agreement, and for each such Data Controller will remain in force as long as Data Processor Processes Personal Data on behalf of Data Controller under the Cloud Subscription License Agreement. By entering into the Cloud Subscription License Agreement with Mattermost, or by providing Personal Data to Mattermost, Data Controller instructs Mattermost to Process such Personal Data.

Instructions on how to execute this DPA with Mattermost

1. This DPA consists of distinct parts: this body and its set of definitions and provisions, the Standard Contractual Clauses, and Appendices 1-2.

2. This DPA has been pre-signed on behalf of Mattermost, Inc., as the data importer.

3. To complete this DPA, Data Controller must: (a) Complete the information in the signature box at the end of the main body of the DPA and sign; (b) Complete the information as the data exporter at the top of Exhibit A (Standard Contractual Clauses); (c) Complete the information in the signature box and sign (i) at the end of the Standard Contractual Clauses and (ii) at the end of each of appendices 1 and 2.

4. Data Controller must send the completed and signed DPA to Mattermost by email, indicating the Data Controller's full entity name in the body of the email, to DPA@mattermost.com. Upon receipt of the validly-completed DPA by Mattermost at this email address, this DPA shall come into effect and legally bind the parties.

For purposes of this DPA, the following definitions shall apply:

"Applicable Data Protection Law" means, in addition to any definitions which may be set out in the Cloud Subscription License Agreement, 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); (iii) the California Consumer Privacy Act of 2018, effective January 1, 2020 (as may be amended from time to time) (the **"CCPA"**); (iv) the UK Data Protection Act (as amended and replaced from time to time); and (v) the Data Protection Acts of the EEA countries (as amended and replaced from time to time).

"**Data Controller**" means the party entering into the Cloud Subscription License Agreement with Mattermost. 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, and includes a "business" as defined in the CCPA.

"Data Processor" has the meaning given in Applicable Data Protection Law (and, for the purposes of this DPA, means Mattermost, Inc.), and includes a "service provider" as defined in the CCPA. Under no circumstances will Data Processor act, or be deemed to act, as a "controller" (or equivalent concept) of the Personal Data under any Applicable Data Protection Law.

"Data Subject" means a natural person whose Personal Data is Processed by Mattermost. Data Subjects include system users of the customer's self-hosted communication system when the system is connected to HPNS and the sharing of Personal Data is enabled. Data Subjects also include persons whose Personal Data is made available to system users and shared by the system users in messages that trigger push notifications.

"EEA" means the European Economic Area.

"Europe" means the EEA and Switzerland.

"Law(s)" means any statute, regulation, ordinance, rule, order, decree, or governmental requirement enacted, promulgated, or imposed by any governmental authority at any level (e.g., municipal, county, province, state or national). Law(s) includes all Applicable Data Protection Laws.

"Cloud Subscription License Agreement" means the agreement between Data Controller and Data Processor for the provision of, and access to, the Service which can be found at https://mattermost.com/cloud-subscription-terms/ unless otherwise agreed upon by the parties.

"Personal Data" means any information that Provider or its Personnel collect, receive or obtain, from or on behalf of Mattermost's customers that (a) relates to an identified or identifiable natural person, or (b) otherwise qualifies as personal data, personal information, or personally identifiable information under one or more of the Privacy Laws. Personal Data may include the following examples, depending on the context: an individual's name, username, social security number, driver's license number, postal address, email address, geolocation, credit account numbers, and vehicle identification number ("VIN"). Personal Data received by HPNS may also be of an arbitrary nature if the customer enables the sending of message preview snippets to HPNS, which allows contents from messages users send to be transmitted.

"Personal Data Breach" means any unauthorized Processing, loss, destruction, use, disclosure, acquisition of, or access to Personal Data.

"Personnel" means any employees, agents, consultants, or contractors of Mattermost.

"Process" or "Processing" means, with respect to Personal Data, any operation or set of operations 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.

"Sub-processor" means any third party data processor engaged by Data Processor 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.

"Supervisor" means any Data Protection Supervisory Authority with competence over Data Controller and Data Processor's Processing of Personal Data.

Mattermost's Obligations.
Mattermost will:
1. Process Personal Data only as necessary to perform its obligations under the Cloud Subscription License Agreement, in compliance with all Applicable Data Protection Laws, and in accordance with Data Controller's documented instructions as set forth in the Cloud Subscription License Agreement and this DPA with regard to transfers of personal data to a third country or an international organization in accordance with Article 28 (3) (a) of the GDPR. Despite the foregoing, Mattermost shall not be required to comply with or observe Data Controller's instructions if such instructions would violate the GDPR or other EU law or EU member state data protection provisions.

2. Implement and maintain appropriate technical and organizational measures to protect Personal Data in accordance with Article 32 of the GDPR against a Personal Data 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 represented by the Processing and the nature of the Personal Data to be protected, including

3. 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 Personal Data Breach affecting Data Controller's Personal Data and to cooperate with Data Controller as necessary to mitigate or remediate the Personal Data Breach;

4. 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 Personal Data Breach under the Applicable Data Protection Law;

5. Taking into account the nature of the Processing, assist Data Controller (including by appropriate technical and organizational measures), insofar as it is commercially reasonable, fulfill 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 In the event 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.

6. Upon request, 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;

7. 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.

Data Controller's Obligations
Data Controller agrees to abide by its obligations under Applicable Data Protection Law.
Data Controller shall, in its use of the Service, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws, including any applicable requirements to provide notice to Data Subjects of the use of Mattermost as Processor. For the avoidance of doubt, Data Controller's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Data Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Data Controller acquired Personal Data. Data Controller specifically acknowledges that its use of the Service will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

Rights of Data Subjects.
Data Subjects may request from Mattermost information as to how Personal Data relating to such Data Subject has been stored, how the Personal Data was collected, and for what purpose. If such Personal Data is incorrect or incomplete, the Data Subject can cause Mattermost to correct or supplement it. The Data Subject may request his/her Personal Data to be deleted if the processing of such Personal Data has no legal basis, or if the legal basis has ceased to apply. The Data Subject may request the identity of the recipient of the Data Subject's Personal Data if such Personal Data has been transmitted to a third party. The Data Subject can object to the processing of his or her Personal Data for purposes of advertising or market/opinion research. The Data Subject may otherwise object to his/her Personal Data being processed, and Mattermost will take such objection into account in relation to all applicable Laws.

Sub-processing of Personal Data.
Data Controller hereby confirms its general written authorization for Mattermost to engage those third-party Sub-processors listed at https://mattermost.com/subprocessors/ in accordance with Article 28 of the GDPR to assist it in providing the Service and Processing Personal Data, provided that such Sub-processors 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 agree to protect the Personal Data to a standard consistent with the requirements of this DPA. 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 Processor shall remain liable to Data Controller for the subcontracted Processing services of any of its Sub-Processors under this DPA.

In the event that Data Controller objects to the Processing of its Personal Data by any newly appointed Sub-processor, 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 not to begin, or to cease further, 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).

Audit
The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: upon Data Controller's written request, and subject to the confidentiality obligations set forth in the Cloud Subscription License Agreement, Mattermost shall make available to Data Controller information regarding Mattermost's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits, to the extent that Mattermost makes them generally available to its customers. Following any notice by Mattermost to Data Controller of an actual or reasonably suspected unauthorized disclosure of Personal Data, upon Data Controller's reasonable belief that Mattermost is in breach of its obligations in respect of protection of Personal Data under this DPA, or if such audit is required by a Supervisor, Data Controller may contact Mattermost in accordance in accordance with the "Notices" Section of the Cloud Subscription License Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data, but only to the extent required under Applicable Data Protection Law. Data Controller shall reimburse Mattermost for any time expended for any such on-site audit at Mattermost's then-current professional services rates, which shall be made available to Data Controller upon request. Before the commencement of any such on-site audit, Data Controller and Mattermost shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Data Controller shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Mattermost. Data Controller shall promptly notify Mattermost and provide information about any actual or suspected non-compliance discovered during an audit. The provision in this section shall by no means derogate from or materially alter the provisions on audits as specified in the Standard Contractual Clauses.

Transfers of Data Received in the European Union.
Data Controller acknowledges that Data Processor and its Sub-processors may maintain data processing operations in countries that are outside of the EEA and Switzerland. As such, Data Processor and its Sub- processors may Process Personal Data in non-EEA and non-Swiss countries. There are multiple HPNS servers available to Mattermost's customers, and the customer can choose servers located in the United States (various locations by connecting to https://hpns.mattermost.com/) or in Germany (Frankfurt by connecting to https://hpns-de.mattermost.com/).

With respect to Personal Data received by Mattermost from the European Union, Mattermost will not transfer Personal Data outside the European Union unless (i) the transferee is located in a country which the European Commission or a national data protection authority has determined to provide an adequate level of protection under EU Data Protection Law or (ii) the transferee has implemented adequate safeguards under EU Data Protection Law such as approved Binding Corporate Rules or Standard Contractual Clauses (the "Clauses"); subject to the following:
1. When used below, the terms "data exporter" and "data importer" shall have the meaning given to them in the Clauses;
2. Data Controller agrees that the audits described in Clauses 5(f) and 12(2) shall be conducted in accordance with the provisions of the Section of this DPA above labeled "Audit".
3. 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 this DPA.
4. 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 section of this DPA labeled "Sub-processing of Personal Data".
5. 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 Cloud Subscription License Agreement. In no event shall any party limit its liability with respect to any Data Subject rights under these Clauses.

Subject Matter of Processing

The Data Processor / Data Importer (where applicable) operates a cloud-based messaging platform, including an online helpdesk ticketing service, cloud-based customer support platform, and customer-support features. In addition, Data Processor / Data Importer operates a self-hosted software system which does not require Data Processor / Data Importer to come in contact with Personal Data from its customers unless customers choose a specific configuration of the system that uses the optional Mattermost Hosted Push Notification Service (HPNS), in lieu of the self-hosted option also offered. HPNS relays mobile push notification messages from the customer's self-hosted server to mobile apps in iTunes and Google Play, which are used by end users on the customer's system. Customers can configure HPNS to share no Personal Data in relaying messages to mobile applications–only notifying users that they have received an alert based on their personal notification preferences–or the customer may choose to enable information that may include the following types of Personal Data: usernames (if Data Controller / Data Exporter enables the feature to display usernames in the HPNS relay), and message preview snippets (which may include Personal Data shared by users in messages, if Data Controller / Data Exporter enables the ability to display message preview snippets for the HPNS relay). While the IP address of the self-hosted server instance is also contained in relay requests, because it does not identify a specific user it is not considered Personal Data in this context. Data subjects include Mattermost's end-users including employees and contractors of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by Mattermost.

Data Subjects

Data Controller / Data Exporter (where applicable) may, at its sole discretion, submit Personal Data to the Service(s), the extent of which is determined and controlled by Data Controller / Data Exporter in compliance with Applicable Data Protection law, and which may include, but is not limited to, the following categories of Data Subjects: employee names, customer names, potential customer names, consultant names, contractor names, and end users.

Categories of Personal Data

Data Controller / Data Exporter (where applicable) may, at its sole discretion, submit Personal Data to the Data Processor / Data Importer through the Service(s), the extent of which is determined and controlled by Data Controller / Data Exporter in compliance with Applicable Data Protection law, and which may concern the following categories and special categories of: usernames, message preview snippets, and possibly racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, health, and sex life.

Limitation of Liability

This DPA shall be subject to the limitations of liability agreed between the Parties in the Cloud Subscription License Agreement. 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 CLOUD SUBSCRIPTION LICENSE AGREEMENT AND THIS DPA SHALL APPLY IN AGGREGATE FOR ALL CLAIMS UNDER BOTH THE CLOUD SUBSCRIPTION LICENSE AGREEMENT AND THIS DPA.

Duration of Processing; Retention of Personal Data.

The duration of the Processing typically happens in less than a fraction of a second between when the Personal Data is received and when it is discarded. Mattermost will not retain your Personal Data longer than necessary to fulfill the purposes for which it is Processed, including the security of our Processing complying with legal and regulatory obligations (e.g. audit, accounting and statutory retention terms), handling disputes, and for the establishment, exercise or defense of legal claims in the countries where Mattermost does business.

Return and Destruction of Personal Data

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 Personal Data, at its expense; or (b) delete all Personal 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 Personal Data stored or Processed by Data Processor on behalf of Data Controller in accordance with Data Processor's deletion policies and procedures, unless otherwise required to store such Personal Data pursuant to applicable law. Data Controller expressly consents to such deletion. If required to store Personal Data, then the Mattermost shall notify Data Controller and continue to safeguard such data in accordance with this DPA.
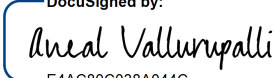
General Provisions
The exclusive jurisdiction for resolving any disputes arising out of this DPA shall be in the courts of San Mateo County, California. Notices under this DPA shall be sent in accordance with the notice provisions of the Cloud Subscription License Agreement. This DPA and the Cloud Subscription License Agreement constitute the entire understanding between the Parties with respect to subject matter herein, and shall supersede any other arrangements, negotiations or discussions between the Parties relating to that subject matter. This DPA may be signed in two or more counterparts, each of which shall be considered an original, and all of which together shall constitute a single instrument.

Contact Information
Any person with questions about this DPA or about Mattermost's handling, Processing or protection Personal Data may contact Mattermost's Privacy Officer at privacy@mattermost.com.

DATA IMPORTER:

Signature: *Aneal Vallurupalli*
DocuSigned by:
E4AC80C038A044C...

Print Name: Aneal Vallurupalli

Title: VP, Finance and Operations

DATA EXPORTER

Signature: _____

Print Name: _____

Title: _____

EXHIBIT A TO DPA
Standard Contractual Clauses

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 organisation: _____

Address: _____

e-mail: _____

(the data exporter)

And

Name of the data importing organisation: Mattermost, Inc.

Address: 530 Lytton Avenue, 2nd Floor, Palo Alto, CA 94301 USA

e-mail: privacy@mattermost.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.

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 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 (1);
(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 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;
(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 exporter 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 Member 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 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 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 organisational 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).

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

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 Clause.

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 (3). 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.
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 the Member State in which the data exporter is established, namely Sweden.
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.

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

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

On behalf of the data importer:

Name (written out in full): Aneal Vallurupalli

Position: VP, Finance and Operations

Email: privacy@mattermost.com

Address: 530 Lytton Avenue, 2nd Floor, Palo Alto, CA 94301 USA

Signature: *Aneal Vallurupalli*
E4AC80C038A044C...

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

Appendix 1 to 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):

Data Importer, Mattermost, Inc., which Processes Personal Data, where such data is Personal Data, upon the instruction of the Data Exporter in accordance with the terms of the Cloud Subscription License Agreement and the DPA.

Data exporter

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

Data Exporter is the legal entity that has executed the DPA based on the Standard Contractual Clauses as a Data Exporter and that has purchased the services of Data Importer on the basis of the Cloud Subscription License Agreement.

Data subjects

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

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: employee names, customer names, potential customer names, consultant names, contractor names, and end users.

Categories of data

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

As set forth in the DPA.

Special categories of data (if appropriate)

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

As set forth in the DPA.

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 the Data Importer is the performance of the Service pursuant to the Cloud Subscription License Agreement.

DATA IMPORTER: **DATA EXPORTER**

Signature: *Aneal Vallurupalli*   Signature: _____
DocuSigned by:
E4AC80C038A044C...

Print Name: Aneal Vallurupalli   Print Name: _____

Title: VP, Finance and Operations   Title: _____

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the 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):

Data importer shall undertake the appropriate technical and organizational security measures designed to protect personal data against the unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These measures should take into account available encryption technology and the costs of implementing the specific measures and must ensure a level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected. Data importer has in place the measures set forth in the Data Protection Addendum.

DATA IMPORTER:

Signature: *Aneal Vallurupalli*
DocuSigned by:
E4AC80C038A044C...

Print Name: Aneal Vallurupalli

Title: VP, Finance and Operations

DATA EXPORTER

Signature: _____

Print Name: _____

Title: _____