Mattermost, Inc.
Data Processing Addendum

This Data Processing Addendum ("DPA") is an addendum to the license agreement ("Agreement") between Mattermost, Inc. ("Mattermost") and the other party entering into the Agreement with Mattermost ("Data Controller"). The terms of this DPA shall only apply to Data Controllers with an active subscription to Mattermost products or service (collectively, the "Service") under an Agreement, and for each such Data Controller will remain in force as long as Mattermost Processes Personal Data on behalf of Data Controller under the Agreement. By entering into the 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 and, as applicable, (i) the controller-to-processor standard contractual clauses approved by the European Commission, including Module Two's obligations in the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("SCCs") in Annex I including its Appendix; and (ii) the International Data Transfer Addendum to the SCCs approved by the United Kingdom's Information Commissioner's Office in Annex II.

2. This DPA has been pre-signed on behalf of Mattermost, Inc.

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) as applicable, complete the information as the data exporter in Annex I in Exhibit B and sign; and (c) complete the information as the data exporter in Exhibit C and sign.

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.

The parties agree as follows:

1. **Definitions.** 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 Agreement, all data protection and data privacy law(s) applicable to the Processing of Personal Data under the Agreement, which may include, but may not be limited to: (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"**) and other U.S. federal or state laws; and (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 Agreement with Mattermost. Any reference to the Data Controller within this DPA, unless otherwise specified, shall include Data Controller and its Affiliates.

   "Data Subject" means a natural person whose Personal Data is Processed by Mattermost. Data Subjects include system users of Data Controller's self-hosted communication system when the system is connected to HPNS and the sharing of Personal Data is enabled. Data Subjects also may 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, the United Kingdom, and Switzerland.
"HPNS" means the Hosted Push Notification Service.

"Personal Data" means any information that Mattermost collects, receives, or obtains from or on behalf of Data Controller under the Agreement 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 Applicable Data Protection Law.

"Personal Data Breach" means a breach of security leading to the accidental, unauthorized, or unlawful loss, destruction, alteration, or disclosure, 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 Mattermost who receives Personal Data from Mattermost for processing on behalf of Data Controller.

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

2. **Role of the Parties.** The parties agree that with respect to Mattermost's Processing of Personal Data, Data Controller is the "business" or "controller" and Mattermost is the "processor" or "service provider", in each case as such terms are defined by Applicable Data Protection Law. In the event Mattermost is required to process Personal Data on the request of an Affiliate of Data Controller, such Affiliate shall also be deemed as the "controller" or "business" as those terms are defined by Applicable Data Protection Law.

3. **Scope of Processing.** The nature, purpose, and duration of the Processing are set forth in the Agreement and in Exhibit A to this DPA.

4. **Compliance.** Mattermost and Data Controller shall comply with Applicable Data Protection Law and shall take steps to protect Personal Data as required by Applicable Data Protection Law. This shall include, but shall not be limited to, Mattermost (i) ensuring that each person Processing Personal Data is subject to a duty of confidentiality with respect to such Personal Data; and (ii) maintaining administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data. Data Controller may take reasonably appropriate steps to ensure that Mattermost Processes Personal Data in a manner consistent with Data Controller's obligations under Applicable Data Protection Law.

   a. ***Data Controller Obligations.*** Data Controller shall, in its use of the Service, Process Personal Data in accordance with the requirements of Applicable Data Protection Law, including any applicable requirements to provide notice to Data Subjects of the use of Mattermost as a "processor" or "service provider". 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 under Applicable Data Protection Law.

   b. ***Mattermost Obligations.*** Mattermost shall provide assistance reasonably necessary for Data Controller to comply with Applicable Data Protection Laws in relation to the Agreement. If Mattermost determines that it can no longer meet its own obligations under Applicable Data Protection Law, Mattermost shall promptly notify Data Controller of such determination. Upon such notice, Data Controller may direct Mattermost to suspend its Processing of Personal Data until Mattermost can meet its material obligations under Applicable Data Protection Law.

5. **Processing of Personal Data.** 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. Mattermost shall

Process Personal Data only as necessary to perform its obligations under the Agreement, in compliance with Applicable Data Protection Law, and in accordance with Data Controller's documented instructions, including as set forth in the Agreement and this DPA, except where otherwise required by law. For the avoidance of doubt, Mattermost will not (i) collect, retain, use, or otherwise disclose Personal Data outside the direct business relationship with Data Controller; (ii) for any purpose other than performing the Processing instructed by Data Controller or as otherwise permitted by Applicable Data Protection Law; (iii) sell Personal Data or share Personal Data for targeted online advertising; or (iv) combine Personal Data with personal data received from another person or persons in any manner not explicitly permitted for a service provider or processor under Applicable Data Protection Law. Mattermost certifies that it understands and will comply with the restrictions of this section.

6. **Instructions for Processing**. Data Controller's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Law. Despite the foregoing, Mattermost shall not be required to comply with or observe Data Controller's instructions if such instructions would violate Applicable Data Protection Law. If Mattermost believes that Data Controller's instructions would violate Applicable Data Protection Law, it will inform Data Controller.

7. **Personal Data Breach.** Mattermost shall notify Data Controller without undue delay in the event of a Personal Data Breach. Mattermost shall also promptly (i) investigate the Personal Data Breach and provide Data Controller with information about the Security Incident; and (ii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach. Notification(s) of Personal Data Breach(es), if any, will be delivered to one or more of Data Controller's business, technical, or administrative contacts by any means Mattermost selects, including via email. It is Data Controller's sole responsibility to ensure it maintains accurate contact information at all times.

8. **Data Subject Requests.** Taking into account the nature of the Processing, Mattermost shall assist Data Controller, insofar as it is commercially reasonable, in fulfilling Data Controller's legal obligation(s) to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law (each a "Data Subject Request"). In the event Mattermost receives a Data Subject Request directly from a Data Subject, it shall (unless prohibited by law) direct the Data Subject to Data Controller in the first instance. In the event Data Controller is unable to fulfill the Data Subject Request, Mattermost, shall, at Data Controller's request and at Data Controller's reasonable expense (scoped prior to Mattermost's response to the Data Subject Request), address the Data Subject Request to the extent required by Applicable Data Protection Law.

9. **Sub-processing of Personal Data.** Data Controller hereby confirms its general written authorization for Mattermost to engage Sub-processors to assist Mattermost in providing the Service and Processing Personal Data, provided that Mattermost agrees to engage a Sub-processor only pursuant to a written contract that contains restrictions on Processing that are consistent with the terms of this DPA. Mattermost may continue to use those Sub-processors already engaged by Mattermost as of the date of this DPA. Mattermost shall make available to Data Controller a current list of Sub-processors at https://mattermost.com/subprocessors/, and Mattermost shall update this list to include any newly appointed Sub-processor at least thirty (30) days prior to the date on which the Sub-processor shall commence processing Personal Data. In the event that Data Controller reasonably objects to the Processing of its Personal Data by any newly appointed Sub-processor, it shall inform Mattermost within fifteen (15) days following the update of the Sub-processor list. In such event, Mattermost will take reasonable steps to address the objections raised by Data Controller and shall inform Data Controller of the steps taken. Such steps may include, for instance, instructing the Sub-processor not to begin, or to cease further, Processing of Data Controller's Personal Data. Mattermost shall remain liable to Data Controller for the subcontracted Processing services of any of its Sub-Processors under this DPA.

10. **Audit._** Upon Data Controller's reasonable written request no more than once a year, and subject to the confidentiality obligations set forth in the Agreement, Mattermost shall make available to Data Controller information necessary: (i) to demonstrate Mattermost's compliance with Applicable Data Protection Law and the obligations set forth in this DPA or (ii) to help Data Controller to conduct any data protection impact assessment or Supervisor consultation it is required to conduct under Applicable Data Protection Law. Mattermost shall allow for and cooperate with reasonable audits by Data Controller or its designated auditor to assess Mattermost's compliance with Applicable Data Protection Law and this DPA. Data Controller may contact Mattermost in accordance with the "Notices" Section of the Agreement to request such an audit. 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 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. As an alternative to Data Controller or its designated auditor conducting such an audit, Mattermost may elect to provide Data Controller, upon Data Controller's request, with a copy of such an audit prepared by a qualified and independent auditor using an appropriate and accepted framework and procedures. In the event that Data Controller becomes aware of unauthorized Processing of Personal Data by Mattermost, Data Controller has the right to take reasonable and appropriate steps to stop and remediate such unauthorized Processing.

11. **European Data Transfers.** This section shall apply to the extent that Mattermost will Process Personal Data originating from Europe to provide the Service. Data Controller acknowledges that Mattermost and its Sub-processors may maintain data processing operations in countries that are outside of Europe. Data Controller (as "data exporter") and Mattermost (as "data importer") hereby enter into controller-to-processor standard contractual clauses approved by the European Commission, including Module Two's obligations in the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "Clauses"), attached as Exhibit B, and the International Data Transfer Addendum to the Clauses approved by the United Kingdom's Information Commissioner's Office, attached as Exhibit C, as supplemented by the terms of this DPA. In the event of a conflict or inconsistency between this DPA and the Clauses, the Clauses shall control solely with respect to Personal Data transferred from Europe to the United States thereunder, provided that:

    (i) Data Controller agrees that the audits described in Clauses 8.9 (c)-(e) shall be conducted in accordance with the provisions of the Section of this DPA above labeled "Audit"; (ii) Data Controller provides a general consent to Mattermost, pursuant to Clause 9(a), to engage onward Sub-processors; (iii) In accordance with the provisions of Clause 9, Data Controller agrees that new Sub-processors may be appointed by Mattermost in accordance with the section of this DPA labeled "Sub-processing of Personal Data"; and (iv) Pursuant to the provisions of Clause 12, any claims brought under the Clauses shall be subject to the terms and conditions set forth in the Agreement.

12. **Limitation of Liability.** This DPA shall be subject to the limitations of liability agreed between the Parties in the Agreement. FOR THE AVOIDANCE OF DOUBT, DATA CONTROLLER ACKNOWLEDGES AND AGREES THAT MATTERMOST'S TOTAL LIABILITY FOR ALL CLAIMS FROM DATA CONTROLLER OR ITS AFFILIATES ARISING OUT OF OR RELATED TO THE AGREEMENT AND THIS DPA SHALL APPLY IN AGGREGATE FOR ALL CLAIMS UNDER BOTH THE AGREEMENT AND THIS DPA.

13. **Return or Destruction of Personal Data.** Upon the termination of Data Controller's access to and use of the Service, Mattermost will, up to sixty (60) days following such termination at the choice of 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. Following such period, Mattermost shall delete all Personal Data Processed by Mattermost on behalf of Data Controller in accordance with Mattermost'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 Mattermost shall notify Data Controller and continue to safeguard such data in accordance with this DPA. This clause does not apply if the parties renew the Agreement for such Personal Data earlier.

14. **General Provisions.** The exclusive jurisdiction for resolving any disputes arising out of this DPA shall be in the courts of San Mateo County, California, United States. Notices under this DPA shall be sent in accordance with the notice provisions of the Agreement. This DPA and the 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.

Mattermost:

Signature: DocuSigned by:
84DCD78B64AC427...

Print Name: Kendra Niedziejko

Title: CFO

12/23/2022

Data Controller

Signature: ____________________________________

Print Name: __________________________________

Title: ____

Exhibit A To DPA: Nature and Purpose of Processing

Subject Matter of Processing

Mattermost operates a cloud-based messaging platform, including an online helpdesk ticketing service, cloud-based customer support platform, and customer-support features. In addition, Mattermost operates a self-hosted software system which does not require Mattermost 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 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 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 generally considered Personal Data in this context.

Data Subjects

Data subjects may include end users of the Service Mattermost provides to Data Controller, including employees, customers, potential customers, consultants, contractors and other end users of Data Controller. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the Service provided by Mattermost.

Categories of Personal Data

The types of Personal Data subject to Processing under this DPA are determined and controlled by Data Controller and may include, depending on the context: an individual's name, username, postal address, email address, and geolocation. Further, racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, health, and sex life, may possibly be Processed. Personal Data received by HPNS may also be of an arbitrary nature if the Data Controller enables the sending of message preview snippets to HPNS, which allows contents from messages users send to be transmitted.

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 retains Personal Data as necessary to fulfill the purposes for which it is Processed, including to maintain the security of its 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.

EXHIBIT B TO DPA: Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(e) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(a) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(b) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(c) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(d) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Has purchased the Services of Data Importer on the basis of the Agreement.

Signature and date:

Role (controller/processor): Controller

Data importer(s):

1. Name: Mattermost, Inc.

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

Contact person's name, position and contact details: Kendra Niedziejko, CFO, privacy@mattermost.com]

Activities relevant to the data transferred under these Clauses: Processing Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement and the DPA

Signature and date: DocuSigned by: 84DCD78B64AC427... 12/27/2022

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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 personal data transferred

As set forth in the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As set forth in the DPA.

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

Continuous.

Nature of the processing

The nature of the processing is the performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

The objective of Processing of Personal Data by the Data Importer is the performance of the Service pursuant to the Agreement.

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

What is set forth in the DPA applies.

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

The sub-processor will Process Personal Data as necessary to provide the Services in accordance to the Agreement. Subject to Section 13 of the DPA, the sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority is determined by the place of establishment of the Data Controller.

A list of supervisory authorities can be found here: https://edpb.europa.eu/about-edpb/about-edpb/members_en
Please note that in Germany, there are several supervisory authorities. The competent regional authority must again be determined by place of establishment: https://www.bfdi.bund.de/EN/Service/Anschriften/Laender/Laender-node.html

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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 take into account available encryption technology and the costs of implementing the specific measures and are designed to 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 following measures:

Security Policies:
Mattermost, Inc. maintains and follows IT security policies and practices that are integral to our business practices, and mandatory for all staff members and contractors. Company policies are reviewed annually and amended as deemed reasonable and are designed to ensure the safety of our customer's data and services.

Penetration Testing:
Mattermost, Inc. conducts annual penetration testing on our software and infrastructure platforms using independent third-parties.

Vulnerability Management:
Mattermost, Inc. conducts regular vulnerability scanning on any production infrastructure using third-party vendors.

User Access Management:
Mattermost, Inc. takes measures to ensure the security of our customer data by following best practices such as role-based access control, principle of least privilege and automatic provisioning and deprovisioning of access. Any actions within the production environments of the company are audited and monitored.

Security Monitoring and Incident Response:
Mattermost, Inc. employs modern security monitoring techniques to detect potential threats to our environments using SIEM and security automation technologies. The company has a staffed 24/7 on-call team for alerts of higher severity or confirmed incidents.

Data Storage and Transit:
Any customer data transfers within Mattermost, Inc. environments are encrypted in transit using modern TLS standards. Any customer data stored within Mattermost, Inc. environments are encrypted at rest using Cloud-provider specific technologies.

Data Portability and Erasure:
Mattermost Cloud customers have full portability of their data and can be provided on request a complete archive for further usage outside of the from us provided environment. After termination of services with

Mattermost, Inc. we will delete any customer instances and related data within 60 days to provide a grace period for restoration of services.

ANNEX III – LIST OF SUB-PROCESSORS

The list of sub-processors is at https://mattermost.com/subprocessors/

EXHIBIT C TO DPA: UK International Data Transfer Addendum

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018
International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date	The start date is the effective date of the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: See Annex I(A) to Exhibit B Trading name (if different): See Annex I(A) to Exhibit B Main address (if a company registered address): See Annex I(A) to Exhibit B Official registration number (if any) (company number or similar identifier): See Annex I(A) to Exhibit B	Full legal name: See Annex I(A) to Exhibit B Trading name (if different): See Annex I(A) to Exhibit B Main address (if a company registered address): See Annex I(A) to Exhibit B Official registration number (if any) (company number or similar identifier): See Annex I(A) to Exhibit B
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: CFO Contact details including email: privacy@mattermost.com
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	X. The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						

2	Yes	No	No	General	30 days	No.
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex I(A) to Exhibit B
Annex 1B: Description of Transfer: See Annex I(B) to Exhibit B
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II to Exhibit B
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III to Exhibit B

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer, to the extent the importer is Controller ☐ Exporter, to the extent the exporter is Controller ☒ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.