(g)   to forward any notification received from the Data Importer or any subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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 subprocessing, 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 subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the Data Importer, or any subprocessor, 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

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the Data Importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2.   The prior written contract between the Data Importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing 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.

4.   The Data Exporter shall keep a list of subprocessing 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 subprocessor 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 subprocessor 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: _____

On behalf of the Data Importer:

Name (written out in full): █████████

Position: █████████

Address: 500 Howard Street, San Francisco, CA 94105, United States of America

Signature: _____

Data Exporter

The Data Exporter is a customer of the Data Importer's communication and productivity software, services, systems and/or technologies, and the Data Exporter is established in the territory of an EU Member State.

Data Importer

The Data Importer is a provider of communication and productivity software, services, systems and/or technologies.

Data subjects

Data Exporter may submit personal data to the Data Importer through the Services, the extent of which is determined and controlled by the Data Exporter in compliance with applicable Data Protection Law and which may include, but is not limited to, personal data relating to the following categories of data subject:

● Authorized Users;
● employees of the Data Exporter;
● consultants of the Data Exporter;
● contractors of the Data Exporter;
● agents of the Data Exporter; and/or
● third parties with which the Data Exporter conducts business.

Categories of data

The personal data transferred concern the following categories of data:

Any personal data comprised in Customer Data. "Customer Data" means all data and information submitted by Authorized Users to the Services and includes message text, files, comments and links, but does not include Non-Slack Products or the Services.

Special categories of data

Data Exporter may submit personal data to the Data Importer through the Services, the extent of which is determined and controlled by the Data Exporter in compliance with Applicable Data Protection Law and which may concern the following special categories of data, if any:

- racial or ethnic origin;

- political opinions;

- religious or philosophical beliefs;

- trade-union membership;

- genetic or biometric data;

- health; and

- sex life.

Processing operations

The personal data transferred will be processed in accordance with the Agreement and any Order Form and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain and update the Services provided to the Data Exporter;

- to provide customer and technical support to the Data Exporter; and

- disclosures in accordance with the Agreement, as compelled by law.

DATA EXPORTER:

Name: _____

Authorised Signature _____

DATA IMPORTER:

Name████████████████

Authorised Signature _____

Technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

The Data Importer has implemented and will maintain appropriate technical and organisational measures to protect the personal data against misuse and accidental loss or destruction as set forth in Slack's Security Practices Datasheet.

DATA EXPORTER:

Name: _____

Authorised Signature _____

DATA IMPORTER:

Name: █████████████

Authorised Signature _____

Annex 2: Slack Master Subscription Agreement

Master Subscription Agreement

This Master Subscription Agreement (this "<u>Agreement</u>") is entered into by and between Slack Technologies Limited, an Irish company with offices at One Park Place, Upper Hatch Street, Dublin 2 ("<u>Slack</u>") and _____ corporation with offices at _____ , effective as of the last date of signature below (the "<u>Effective Date</u>").

1. **Definitions**

    "**Affiliate**" means any entity which directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

    "**Authorized User**" means an individual who is authorized by Customer to use the Services under Customer's account, and who has been supplied a user identification and password.

Authorized Users may include, for example, Customer's employees, consultants, contractors and agents, and third parties with which Customer transacts business.

"**Beta Services**" means Services, features or functionality that Slack may make available to Customer to try, at its option, and which may be designated by Slack as a beta, pilot, limited release, developer preview, non-production, evaluation, or by a similar description.

"**Customer**" means the customer named above and those of its Affiliates that have entered into Order Forms for the purchase of Services under this Agreement.

"**Customer Data**" means all content and information submitted by Authorized Users to the Services, such as messages or files, comments, and links, but does not include Non-Slack Products or the Services.

"**Documentation**" means Slack's online user guides, and policies, as updated from time to time, accessible via slack.com/help or such successor site.

"**Non-Slack Products**" means online applications and offline software products that interoperate with the Services and are provided by Customer, a third-party or, are listed on the Slack App Directory.

"**Order Form**" means an ordering document (including any online order) specifying the Services to be provided hereunder that is entered into between Customer and Slack or any of Slack's Affiliates. By entering into an Order Form hereunder, an Affiliate agrees to be bound by the terms of this Agreement as if it were an original party hereto.

"**Services**" means Slack's communication and collaboration software-as-a-service products that connect Authorized Users, content, information, and Non-Slack Products, including Slack's desktop and mobile applications. "Services" exclude Non-Slack Products.

"**Slack App Directory**" means an online directory of applications that interoperate with the Services.

2. **Slack Responsibilities**

2.1. **Provision of Services.** Slack will (a) make the Services purchased under an Order Form available to Customer pursuant to this Agreement; and (b) provide the Services in accordance with any applicable uptime commitments set forth in the Documentation, but will in no event, use less than commercially reasonable efforts to make the Services available 24 hours a day, 7 days a week, except for planned downtime of which, to the extent exceeding five continuous minutes, Slack gives at least 48 hours' notice via the Services.

2.2. **Performance and Features.** Slack warrants that (a) the Services will perform materially in accordance with the applicable Documentation; and (b) subject to the "Non-Slack Products" section, Slack will not materially decrease the functionality of the Services during a subscription term. For any breach of an above warranty, Customer's exclusive remedies are those described in the sections titled "Termination for Cause" and "Refund or Payment upon Termination."

2.3. **Protection of Customer Data.** Slack will maintain administrative, physical, and technical safeguards for the security, confidentiality and integrity of Customer Data at a level not materially less protective than as described in https://slack.com/security-practices, as updated from time-to-time ("**Security Practices Page**"). Those safeguards will include measures for preventing unauthorized access, use, modification, deletion and disclosure of Customer Data by Slack personnel. Before providing necessary access to Customer Data to a third-party service provider, Slack will ensure that the third-party maintains reasonable data practices for maintaining the confidentiality and security of the Customer Data and preventing unauthorized access to or use of the Customer Data. However, Customer (not Slack) bears sole responsibility for adequate security, protection and backup of Customer Data when in Customer's or its

1

representatives or agents' possession or control.

2.4. Slack Personnel. Slack will be responsible for the performance of Slack's personnel (including Slack's employees and independent contractors) and their compliance with Slack's obligations under this Agreement, except as otherwise specified herein.

2.5. Compliance with Laws. Slack will comply with laws applicable to Slack in its provisioning of the Services to its customers generally (i.e. without regard to the nature of the Customer Data and/or Customer's particular use or configuration of the Services).

3. Access and Use of the Services.

3.1. Account Creation and Subscriptions. Customer will identify a primary owner for its account. Customer may use its primary owner credentials to create other owner accounts, admin accounts and standard user accounts for its Authorized Users. Unless otherwise specified in an applicable Order Form, (a) Services are purchased as Authorized User subscriptions; (b) additional Authorized User subscriptions may be added via the Services interface by Customer or by Order Form during the applicable subscription term at the same pricing as that for the pre-existing subscriptions thereunder, prorated for the remainder of the subscription term in effect at the time the additional Authorized User subscriptions are added; and (c) all Authorized User subscriptions will terminate on the same date.

3.2. Usage Limits. Authorized User subscriptions cannot be shared or used by more than one Authorized User. Customer is responsible for maintaining the confidentiality of its logins, passwords and accounts and for all activities that occur under its accounts. Customer may refer to the Documentation for additional information on Slack's policies, storage limitations, and such other notices Slack publishes in connection with the Services from time-to-time.

3.3. Customer Responsibilities. Customer will (a) obtain any permissions required for Customer's owners and administrators to have the rights to access Customer Data in connection with the Services; (b) be responsible for Authorized Users' compliance with this Agreement; (c) be responsible for the accuracy, appropriateness and legality of Customer Data; (d) use commercially reasonable efforts to prevent unauthorized access to or use of Services, and notify Slack promptly of any such unauthorized access or use; and (e) use the Services only in accordance with applicable laws and government regulations.

3.4. Usage Restrictions. Customer may not (a) make the Services available to, or use the Services for the benefit of, anyone other than Customer or those Authorized Users directly supporting Customer; (b) upload, post, transmit, or otherwise make available to the Services any content that (i) is unlawful or tortious, or (ii) Customer does not have a right to make available under any applicable law or under contractual or fiduciary relationships, or that infringes any patent, trademark, trade secret, copyright or other proprietary rights; (c) sublicense, resell, time share or similarly exploit the Services; (d) upload, post, transmit, or otherwise make available any content or information designed to interrupt, interfere with, destroy or limit the functionality of any computer software or hardware or telecommunications equipment; (e) reverse engineer, modify, adapt, or hack the Services, or otherwise attempt to gain unauthorized access to the Services or its related systems or networks; or (f) access the Services or the Documentation to build a competitive product or service.

3.5. No Health Information. In the unlikely event that Customer is subject to the US Health Insurance Portability and Accountability Act and related amendments and regulations as updated or replaced ("HIPAA"), Customer acknowledges that Slack is not a Business Associate or subcontractor (as those terms are defined in HIPAA) and that the Services are not HIPAA compliant. Customer must not submit, collect or use any "protected health information" as defined in 45 CFR §160.103 ("PHI"), with or to the Services, unless and until a business associate agreement is executed and Customer is in compliance with the obligations therein.

3.6. Removal Requests. If Slack reasonably believes that it is required to remove any Customer Data or a Non-Slack Product, or receives information that Customer Data or a Non-Slack Product may violate applicable law or rights of a third-party, Customer will promptly remove such Customer Data from its systems upon written notice from Slack (via email to Customer's