Terms & Policies

Data Processing Addendum

INTERCOM

This Data Processing Addendum, including its annexes and the Standard Contractual Clauses, ("DPA") is made by and between Intercom (“Intercom”), and Customer, pursuant to the Master SaaS Subscription Agreement, the Subscription Terms of Service or other written or electronic agreement between the parties (as applicable) ("Agreement").

This DPA forms part of the Agreement and sets out the terms that apply when Personal Data is processed by Intercom under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data is processed.

1. **Definitions.** Any capitalized term used but not defined in this DPA has the meaning provided to it in the Agreement.

i. **"Account Data"** means Personal Data that relates to Customer’s relationship with Intercom, including to access Customer’s account and billing information, identity verification, maintain or improve performance of the Services, provide support, investigate and prevent system abuse, or fulfill legal obligations.

ii. **"Affiliate"** means any entity controlled by, controlling or under common control by an entity, where "control" means ownership of or the right to control greater than 50% of the voting securities of such entity.

iii. **"Applicable Data Protection Legislation"** refers to laws and regulations applicable to Intercom's processing of personal data under the Agreement, including but not limited to (a) the GDPR, (b) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2019 (**"UK GDPR"**) and the Data Protection Act 2018 (together, **"UK Data Protection Laws"**), (c) the Swiss Federal Data Protection Act and its implementing regulations (**"Swiss DPA"**), (d) CCPA, and (e) Australian Privacy Principles and the Australian Privacy Act (1988), in each case, as may be amended, superseded or replaced.

iv. **"CCPA"** means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder, in each case, as may be amended from time to time. This includes but it is not limited to the California Privacy Rights Act of 2020.

v. **"Controller"** or **"controller"** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

vi. **"Customer Data"** means personal data that relates to Customer's relationship with Intercom, including Personal Data that Intercom processes as a Processor on behalf of Customer.

vii. **"Europe"** means for the purposes of this DPA the European Economic Area (**"EEA"**), United Kingdom (**"UK"**) and Switzerland.

viii. **"GDPR"** means Regulation 2016/679 of the European Parliament and of the Council 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).

ix. **"Personal Data"** or **"personal data"** means any information, including personal information, relating to an identified or identifiable natural person ("data subject") or as defined in and subject to Applicable Data Protection Legislation.

x. "Privacy Policy" means the then-current privacy policy for the Services available at https://www.intercom.com/legal/privacy.

xi. **"Processor"** or **"processor"** means the entity which processes Personal Data on behalf of the Controller.

xii. **"Processing"** or **"processing"** (and **"Process"** or **"process"**) means any operation or set of operations performed upon Personal Data, whether or not by automated means, means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

xiii. **"Restricted Transfer"** means: (i) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

xiv. **"Security Breach"** means a breach of security leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data transmitted, stored or otherwise processed by Intercom. A Security Incident shall not include an unsuccessful attempt or activity that does not compromise the security of Customer Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

xv. **"Standard Contractual Clauses"** or **"SCCs"** means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or (d) where the UK GDPR means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein ("UK SCCs") and (iii) where

the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs") (in each case, as updated, amended or superseded from time to time).

xvi. **"Sub-processor"** or **"sub-processor"** means (a) Intercom, when Intercom is processing Customer Data and where Customer is itself a processor of such Customer Data, or (b) any third-party Processor engaged by Intercom or its Affiliates to assist in fulfilling Intercom's obligations under the Agreement and which processes Customer Data. Sub-processors may include third parties or Intercom Affiliates but shall exclude Intercom employees, contractors or consultants.

xvii. **"Third Party Request"** means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

xviii. "UK Addendum" means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein. This is found in Schedule 4 below.

2. **Applicability and Scope.**

i. Applicability. This DPA will apply only to the extent that Intercom processes, on behalf of Customer, Personal Data to which Applicable Data Protection Legislation applies.

ii. Scope. The subject matter of the data processing is the provision of the Services, and the processing will be carried out for the duration of the Agreement. Schedule 1 (Details of Processing) sets out the nature and purpose of the processing, the types of Personal Data Intercom processes and the categories of data subjects whose Personal Data is processed.

iii. Intercom as a Processor. The parties acknowledge and agree that regarding the processing of Customer Data, Customer may act either as a controller or processor and Intercom is a processor. Intercom will process Customer Data in accordance with Customer’s instructions as set forth in Section 3 (Customer Instructions).

iv. Intercom as a Controller of Account Data. The parties acknowledge that, regarding the processing of Account Data, Customer is a controller and Intercom is an independent controller, not a joint controller with Customer. Intercom will process Account Data as a controller (a) in order to manage the relationship with Customer; (b) carry out Intercom's core business operations; (c) in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) identity verification; (e) to comply with Intercom's legal or regulatory obligations; and (f) as otherwise permitted under Applicable Data Protection Legislation and in accordance with this DPA, the Agreement, and the Privacy Policy.

3. **Intercom as a Processor – Processing Customer Data.**

i. Customer Instructions. Customer appoints Intercom as a processor to process Customer Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents, and detecting and preventing exploits or abuse); (b) as necessary to comply with applicable law, including Applicable Data Protection Legislation; and (c) as otherwise agreed in writing between the parties ("Permitted Purposes").

ii. Lawfulness of Instructions. Customer will ensure that its instructions comply with Applicable Data Protection Legislation. Customer acknowledges that Intercom is neither responsible for determining which laws are applicable to Customer's business nor whether Intercom's Services meet or will meet the requirements of such laws. Customer will ensure that Intercom's processing of Customer Data, when done in accordance with Customer's instructions, will not cause Intercom to violate any applicable law, including Applicable Data Protection Legislation. Intercom will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate applicable law, including Applicable Data Protection Legislation.

iii. Additional Instructions. Additional instructions outside the scope of the Agreement or this DPA will be mutually agreed to between the parties in writing.

4. **Purpose Limitation.** Intercom will process Personal Data in order to provide the Services in accordance with the Agreement. Schedule 1 (Details of Processing) of this DPA further specifies the nature and purpose of the processing, the

processing activities, the duration of the processing, the types of Personal Data and categories of data subjects.

5. **Compliance.** Customer shall be responsible for ensuring that: a) all such notices have been given, and all such authorizations have been obtained, as required under Applicable Data Protection Legislation, for Intercom (and its Affiliates and Sub-processors) to process Customer Data as contemplated by the Agreement and this DPA; b) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including Applicable Data Protection Legislation; and c) it has, and will continue to have, the right to transfer, or provide access to, Customer Data to Intercom for processing in accordance with the terms of the Agreement and this DPA.

6. **Confidentiality.**

i. Confidentiality Obligations of Intercom Personnel.

a. Security Policy and Confidentiality. Intercom requires all employees to acknowledge in writing, at the time of hire, they will adhere to terms that are in accordance with Intercom's security policy and to protect Customer Data at all times. Intercom requires all employees to sign a confidentiality statement at the time of hire.

b. Intercom will ensure that any person that it authorizes to process Customer Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality (whether in accordance with Intercom's confidentiality obligations in the Agreement or a statutory duty).

c. Background Checks. Intercom conducts at its expense a criminal background investigation on all employees who are to perform material aspects of the Services under this Agreement.

ii. Responding to Third Party Requests. In the event any Third Party Request is made directly to Intercom in connection with Intercom's processing of Customer Data, Intercom will promptly inform Customer and provide details of the same, to the extent legally permitted. Intercom will not respond to any Third Party Request, without prior notice to Customer and an opportunity to object, except as legally required to do so or to confirm that such Third Party Request relates to Customer.

7. **Sub-processors.**

i. Authorization for Sub-processing. Customer agrees that (a) Intercom may engage Sub-processors as listed at https://www.intercom.com/legal/security-third-parties (the "Sub-processor Page") which may be updated from time to time and Intercom Affiliates; and (b) such Affiliates and Sub-processors respectively may engage third party processors to process Customer Data on Intercom's behalf. Customer provides a general authorization for Intercom to engage onward sub-processors that is conditioned on the following requirements: (a) Intercom will restrict the onward sub-processor's access to Customer Data only to what is strictly necessary to provide the Services, and Intercom will prohibit the sub-processor from processing the Personal Data for any other purpose. (b) Intercom agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation; and (c) Intercom will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.

ii. Current Sub-processors and Notification of Sub-processor Additions.

a. Customer understands that effective operation of the Services may require the transfer of Customer Data to Intercom Affiliates, such as Intercom, Inc., or to Intercom's Sub-processors, see Schedule 3. Customer hereby authorizes the transfer of Customer Data to locations outside Europe (Intercom's primary processing facilities are in the United States of America), including to Intercom Affiliates and Sub-processors, subject to continued compliance with this DPA throughout the duration of the Agreement. Customer hereby provides general authorization to Intercom engaging additional third-party Sub-processors to process Customer Data within the Services for the Permitted Purposes.

b. Intercom may, by giving reasonable notice to the Customer, add to the Sub-processor Page. Intercom will notify Customer if it intends to add or replace Sub-processors from the Sub-Processor Page at least 10 days prior to any such changes. To receive such notification, Customers can follow link http://privacy.intercom.com/third-party-subscribe to join Intercom's distribution list. If Customer objects to the appointment of an additional Sub-processor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, then Intercom will work in good faith with Customer to find an alternative solution. In the event that the parties are unable to

find such a solution, Customer may terminate the Agreement at no additional cost.

8. **Impact Assessments and Consultations.** Intercom shall, to the extent required by Applicable Data Protection Legislation, provide Customer with reasonable assistance (at Customer's cost and expense) with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under such legislation.

9. **Security.**

i. Intercom has in place and will maintain throughout the term of this Agreement appropriate technical and organizational measures designed to protect Customer Data against Security Breaches.

ii. These measures shall at a minimum comply with applicable law and include the measures identified in Schedule 2 (Technical and Organizational Security Measures).

iii. Customer acknowledges that the security measures are subject to technical progress and development and that Intercom may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

iv. Intercom will ensure that any person authorized to process Customer Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality.

v. Upon becoming aware of a Security Breach involving Customer Data processed by Intercom on behalf of Customer under this DPA, Intercom shall notify Customer without undue delay and shall provide such information as Customer may reasonably require, including to enable Customer to fulfil its data breach reporting obligations under Applicable Data Protection Legislation.

vi. Intercom’s notification of or response to a Security Breach shall not be construed as an acknowledgement by Intercom of any fault or liability with respect to the Security Breach.

vii. Customer is solely responsible for its use of the Service, including (a) making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of Customer Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Service; and (c) backing up Customer Data.

10. **Return or Deletion of Customer Data.** Upon termination or expiry of this Agreement, Intercom will (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control as soon as reasonably practicable and within a maximum period of 30 days of termination or expiry of the Agreement, save that this requirement will not apply to the extent that Intercom is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Intercom will securely isolate and protect from any further processing, except to the extent required by applicable law.

11. **Audits.**

i. The parties acknowledge that when Intercom is acting as a processor on behalf of Customer, Customer must be able to assess Intercom’s compliance with its obligations under Applicable Data Protection Legislation and this DPA.

ii. Intercom shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and the obligations under Article 28 of the GDPR. While it is the parties' intention ordinarily to rely on the provision of the documentation to demonstrate Intercom's compliance with this DPA and the provisions of Article 28 of the GDPR, Intercom shall permit Customer (or its appointed third party auditors) to carry out an audit at Customer’s cost and expense (including without limitation the costs and expenses of Intercom) of Intercom’s processing of Customer Data under the Agreement following a Security Breach suffered by Intercom, or upon the instruction of a data protection authority acting pursuant to Applicable Data Protection Legislation. Customer must give Intercom reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Intercom's operations. Any such audit shall be subject to Intercom's security and confidentiality terms and guidelines and may only be performed a maximum of once annually. If Intercom declines to follow any

instruction requested by Customer regarding audits, Customer is entitled to terminate the Agreement.

iii. Intercom uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Data. A description of Intercom's certifications and standards for audit can be found at https://www.intercom.com/security.

12. **Transfer Mechanisms.**

i. Location of Processing. Customer acknowledges that Intercom and its Sub-processors may transfer and process personal data to and in the United States of America and other locations in which Intercom, its Affiliates or its Sub-processors maintain data processing operations, as more particularly described in the Sub-processor Page. Intercom shall ensure that such transfers are made in compliance with Applicable Data Protection Legislation and this DPA.

ii. Transfer Mechanism. The parties agree that when the transfer of personal data from Customer (as "data exporter") to Intercom (as "data importer") is a Restricted Transfer and Applicable Data Protection Legislation require that appropriate safeguards are put in place, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this DPA, as follows:

a. In relation to transfers of Customer Data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:

1. Module Two or Module Three will apply (as applicable);
2. in Clause 7, the optional docking clause will apply;
3. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in section 7.ii.b of this DPA;
4. in Clause 11, the optional language will not apply;
5. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by by the law of the EU Member State in which the data exporter is established and if no such law by Irish law;
6. in Clause 18(b), disputes shall be resolved before the courts of the EU Member State in which the data exporter is established and otherwise Ireland;

7. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and
8. Subject to section 9.iii of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA;

b. In relation to transfers of Account Data protected by the GDPR and processed in accordance with Section 2.iv of this DPA, the EU SCCs shall apply, completed as follows:

1. Module One will apply;
2. in Clause 7, the optional docking clause will apply;
3. in Clause 11, the optional language will not apply;
4. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
5. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
6. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and
7. Subject to section 9.iii of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA;

c. In relation to transfers of personal data protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under sub-paragraphs (a) and (b) above will apply with the following modifications:

1. references to "Regulation (EU) 2016/679" shall be interpreted as references to UK Privacy Laws or the Swiss DPA (as applicable);
2. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Privacy Laws or the Swiss DPA (as applicable);
3. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);
4. the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);

5. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the UK Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);
6. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);
7. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and
8. with respect to transfers to which UK Privacy Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

d. To the extent that and for so long as the EU SCCs as implemented in accordance with sub-paragraph (a)-(c) above cannot be used to lawfully transfer Customer Data and Account Data in accordance with the UK GDPR to Intercom, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Schedules 1 and 2 of this DPA.

1. in relation to data that is protected by the UK GDPR, the EU SCCs will apply as follows: (i) apply as completed in accordance with paragraph 7(a) above; and (ii) be deemed amended as specified by Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this DPA. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule I and Schedule II of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

e. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the

Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

iii. Alternative Transfer Mechanism. To the extent that Intercom adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Applicable Data Protection Legislation) (**"Alternative Transfer Mechanism"**), the Alternative Transfer Mechanism shall upon notice to Customer and an opportunity to object, apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Legislation applicable to Europe and extends to territories to which Customer Data and Account Data is transferred).

13. **Cooperation and Data Subject Rights.**

i. Data Subject Rights. Intercom shall, taking into account the nature of the processing, provide reasonable assistance to Customer where possible and at Customer's cost and expense, to enable Customer to respond to requests from a data subject seeking to exercise their rights under Applicable Data Protection Legislation. In the event that such request is made directly to Intercom, if Intercom can, through reasonable means, identify the Customer as the controller of the Personal Data of a data subject, Intercom shall promptly inform Customer of the same

ii. Cooperation. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Legislation or (b) any Third Party Request relating to the processing of Account Data or Customer Data conducted by the other party, such party will promptly inform the other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Legislation.

14. **Miscellaneous.**

i. If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail. The order of precedence will be: (a) this DPA; (a) the Agreement; and (c) the Privacy Policy. To the extent there is any conflict between the Standard

Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Pol-icy, the provisions of the Standard Contractual Clauses will prevail.

ii. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

iii. In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

iv. In the event (and to the extent only) of a conflict (whether actual or perceived) among Applicable Data Protection Legislation, the parties (or relevant party as the case may be) shall comply with the more onerous requirement or standard which shall, in the event of a dispute in that regard, be solely determined by Intercom.

v. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Sections 2(iii) and 2 (iv), Intercom reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation.

vi. Except as amended by this DPA, the Agreement will remain in full force and effect.

vii. Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that Intercom access to Customer Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

viii. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

ix. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.

The parties have caused this DPA to be executed by their authorized representatives, and this DPA, including its annexes and the Standard Contractual Clauses, will be effective on the date both parties have signed it.

Signed on behalf of Customer	**Signed on behalf of Intercom**
Company Legal Name:	Intercom
Signed:	Signed:
Name:	Name:
Title:	Title:
Date:	Date:

Schedule 1

DETAILS OF PROCESSING

Annex I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name of Data exporter:	The party identified as the "Customer" in the Agreement and this DPA
Address:	As set forth in the Agreement
Contact person's name, position, and contact details:	As set forth in the Agreement

Activities relevant to the data transferred under these Clauses:	See Annex 1(B) below
Signature and date:	This Annex I shall automatically be deemed executed when the Agreement is executed by Customer
Role (controller/processor):	Controller or Processor

Data importer(s): [*Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

Name:	As set forth in the Agreement
Address:	As set forth in the Agreement
Contact person's name, position, and contact details:	Intercom Privacy Team – legal@intercom.io
Activities relevant to the data transferred under these Clauses:	See Annex 1(B) below
Signature and date:	This Annex I shall automatically be deemed executed when the Agreement is executed by Intercom.
Role (controller/processor):	Processor

B. DESCRIPTION OF PROCESSING/ TRANSFER

Categories of Data Subjects whose personal	**Module One** Customer's employees and individuals authorized by Customer to access Customer's Intercom account:

data is transferred	Employees or contact persons of Customer's prospects, customers, business partners and vendors.
	Modules Two and Three Customer's end users: Prospects, customers, business partners and vendors of Customer (who are natural persons).
Categories of Personal Data transferred	**Module One** Account Data which constitutes Personal Data, such as name and contact information as well as Customer billing address.
	Modules Two and Three Any Customer Data processed by Intercom in connection with the Services and which could constitute any type of Personal Data included in chats or messages, including, without limitation, username, password, email address, IP address as well as customer attribute data, website page view data, click data and social media information.
Sensitive data transferred (if applicable) and applied restrictions or safeguards	Intercom does not knowingly collect (and Customer shall not submit) any sensitive data or any special categories of data (as defined under Applicable Data Protection Legislation).
Frequency of the transfer	Continuous.
Nature and purpose(s) of the data transfer and Processing	**Module One** Personal data contained in Account Data will be processed to manage the account, including to access Customer's account and billing information, for identity verification, to maintain or improve the performance of

	the Services, to provide support, to investigate and prevent system abuse, or to fulfill legal obligations.
	Modules Two and Three Personal Data contained in Customer Data will be subject to the following basic processing activities: Intercom provides a communication platform to facilitate interaction and engagement between the Customer and end users. This service will consist of providing a communication platform for the Customer to use in order to on-board and retain end users as well as analyze their use of the Customer's product and/or services. Intercom will process personal data as necessary to provide the Services under the Agreement. Intercom does not sell Customer's Personal Data or Customer end users' Personal Data and does not share such end users' Personal Data with third parties for compensation or for those third parties' own business interests. Additional details about Intercom's products and services can be found at https://www.intercom.com.
Retention period (or, if not possible to determine, the criterial used to determine the period)	**Module One** Intercom will process Account Data as long as required (a) to provide the Services to Customer; (b) for Intercom's lawful and legitimate business needs; or (c) in accordance with applicable law or regulation. Account Data will be stored in accordance with the Privacy Policy.
	Modules Two and Three Upon termination or expiry of this Agreement, Intercom will (at Customer's election) delete or return to Customer all Customer Data (including copies) in its

	possession or control as soon as reasonably practicable and within a maximum period of 30 days of termination or expiry of the Agreement, save that this requirement will not apply to the extent that Intercom is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Intercom will securely isolate and protect from any further processing, except to the extent required by applicable law.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing	**Modules Two and Three only** Intercom will restrict the onward sub-processor's access to Customer Data only to what is strictly necessary to provide the Services, and Intercom will prohibit the sub-processor from processing the Personal Data for any other purpose. Intercom imposes contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation. Intercom will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.
Identify the competent supervisory authority/ies in accordance with Clause 13	Where the EU GDPR applies, the competent supervisory authority shall be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are

	located.. Where the UK GDPR applies, the UK Information Commissioner's Office.

Schedule 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Annex II

Further details of Intercom's technical and organizational security measures to protect Customer Data are available at:

- https://www.intercom.com/security
- https://www.intercom.com/legal/security-policy
- https://intercom.com/help/en/articles/1385437-how-intercom-complies-with-gdpr
- https://www.intercom.com/legal/privacy

Where applicable, this Schedule 2 will serve as Annex II to the Standard Contractual Clauses. The following table provides more information regarding the technical and organizational security measures set forth below.

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security M
Measures of pseudonymisation and encryption of personal data	• All data sent to or from Intercom is encrypted in 1.2. • Customer Personal Data is encrypted at rest usin encryption, leveraging AWS' encryption framewo described in https://d0.awsstatic.com/whitepape data-at-rest-with-encryption.pdf • All Intercom datastores used to process Custome configured and patched using commercially reas according to industry-recognized system-harder • See "Encryption" at https://www.intercom.com/s

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Intercom has implemented a formal procedure fo security events. When security events are detect escalated to an emergency alias, relevant parties notified, and assembled to rapidly address the ev security event is contained and mitigated, releva a post-mortem analysis, which is reviewed in per distributed across the company and includes act make the detection and prevention of a similar e future. • All Customer Data is permanently stored in the U up for disaster recovery. • Intercom relies on Amazon Web Services (AWS), Infrastructure-As-A-Service provider. Intercom l portfolio of globally redundant services to ensure reliably. Intercom benefits from the ability to dyn or completely re-provision its infrastructure reso needed basis, across multiple geographical areas vendor, tools, and APIs. Intercom's infrastructure down on demand as part of day-to-day operation response to any changes in our customers' needs not just compute resources, but storage and data networking, security, and DNS. Every componen infrastructure is designed and built for high avail • Intercom's data security, high availability, and bu are designed to ensure application availability an information from accidental loss or destruction. I Disaster Recovery plan incorporates geographic its 3 U.S. data centers. Subscription Service resto commercially reasonable efforts and is performe with AWS' ability to provide adequate infrastruct prevailing failover location. All of Intercom recov mechanisms are tested regularly and processes a required. • Intercom operates a dedicated 24x7 on-call incid function, ready to immediately respond to, and m Customer impacting issues. This is supported by

	broader internal Availability program which is de ensuring Intercom maintains their system availab • Intercom has no direct reliance on specific office sustain operations. All operational access to proc can be exercised at any location on the Internet. leverages a range of best-of- breed technologies cloud tools to deliver uninterrupted remote work • All Customer Data deleted by Intercom is delete datastores in accordance with the NIST Special F 88 Revision 1, Guidelines for Media Sanitation De (available at http://nvlpubs.nist.gov/nistpubs/SpecialPublicat 88r1.pdf). With respect to Customer Data encryp with this security policy, this deletion may be dor and securely deleting all copies of the keys used • See "Back Ups and Monitoring" at www.intercom
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• See response for "*Measures for ensuring ongoing integrity, availability and resilience of processing services*" above.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	• Intercom regularly tests their security systems ar ensure they meet the requirements of this securi ensures that the physical and environmental secu audited for SOC 2 Type II compliance, among otl • Application Scans. Intercom performs periodic (l once per month) application vulnerability scans. shall be remediated on a risk basis. • Third party penetration tests. Intercom employs third-party vendor to conduct periodic (but no le year) penetration tests on their web properties.

	• Bug bounty program. Intercom maintains a secur program, which gives independent security resea for testing and submitting vulnerability reports.
Measures for user identification and authorisation	• Single Sign-On (SSO) • Logical Access Controls. Intercom assigns a uniq employee and leverages an Identity Provider to r systems processing Customer Data. • All access to systems processing Customer Data Multi Factor Authentication (MFA). • Intercom restricts access to Customer Data to or with a “need-to-know” for a Permitted Purpose a privileges principles. • Intercom regularly reviews at least every 180 day and systems with access to Customer Data and r upon termination of employment or a change in j results in employees no longer requiring access t • Intercom mandates and ensures the use of syste “strong passwords” in accordance with the best p (described below) on all systems hosting, storing that have or control access to Customer Data and all passwords and access credentials are kept co shared among personnel. • Password best practices implemented by Interco Provider. Passwords must meet the following crit least 10 characters; b. must contain lowercase an letters, numbers, and a special character; c. cann vendor provided list of common passwords. • Intercom maintains and enforces “account lockou accounts with access to Customer Data when an more than ten (10) consecutive incorrect passwo • Intercom does not operate any internal corporate access to Intercom resources is protected by stro and MFA. • Intercom monitors their production systems and maintains security controls and procedures desig

	detect, and respond to identified threats and risk • Strict privacy controls exist in the application coc designed to ensure data privacy and to prevent c accessing another customer's data (i.e., logical se
Measures for the protection of data during transmission	• See "*Measures of pseudonymisation and encrypt data*" above. • See "Infrastructure" at www.intercom.com/legal/
Measures for the protection of data during storage	• Intrusion Prevention. Intercom implements and r working network firewall to protect data accessib and will keep all Customer Data protected by the times. • Intercom keeps its systems and software up to da upgrades, updates, bug fixes, new versions, and c modifications necessary to ensure security of the • Security Awareness Training. Intercom requires a privacy training for all employees with access to • Intercom uses anti-malware software and keeps t software up to date. Customer instances are logi and attempts to access data outside allowed dor are prevented and logged. • Endpoint security software • System inputs recorded via log files • Access Control Lists (ACL) • Multi-factor Authentication (MFA) • See "Back Ups and Monitoring" and "Permissions Authentication" at https://www.intercom.com/se
Measures for ensuring physical security of locations at which personal data are processed	• Physical Access Control. Intercom's services and in AWS' facilities in the USA and protected by AV with their security protocols. • Access only to approved personnel.

	• All personnel who need data center access must access and provide a valid business justification. are granted based on the principle of least privile bound. Requests are reviewed and approved by personnel, and access is revoked after the reque
Measures for ensuring events logging	• See "Measures for the protection of data during • See https://www.intercom.com/help/en/articles/ actions-taken-in-your-workspace-with-teammat
Measures for ensuring system configuration, including default configuration	• Change and Configuration Management. Interco continuous automation for application and opera deployment for new releases. Integration testing are done upon every build with safeguards in pla and reliability. Intercom has a process for critical that can be deployed to Customers within minut Intercom can roll out security updates as require criticality. • Access Control Policy and Procedures • Change Management Procedures
Measures for internal IT and IT security governance and management	• Information security management procedures in the ISO 27001:2013 standard. • Information-related business operations continu in accordance with the ISO27001:2013 standard. • Information security policy • Security Breach Response Plan • Other written security policies include: (a) Busin Policy; (b) Secure Software Development Policy; Device Policy; (d) Data Classification Policy; (e) N Policy; (f) IT Security Policy; (g) Physical Security Control Policy.
Measures for certification/assurance	• See https://www.intercom.com/security.

of processes and products	
Measures for ensuring data minimisation	• Data collection is limited to the purposes of proc data that the Customer chooses to provide). • Security measures are in place to provide only th amount of access (least privilege) necessary to p functions. • Upon termination or expiry of this Agreement, In Customer's election) delete or return to Custom Data (including copies) in its possession or contr reasonably practicable and within a maximum pe termination or expiry of the Agreement, save tha will not apply to the extent that Intercom is requi law to retain some or all of the Customer Data, or Data it has archived on back-up systems, which C Intercom will securely isolate and protect from ar processing, except to the extent required by app • More information about how Intercom processes set forth in the Privacy Policy available at https://www.intercom.com/legal/privacy.
Measures for ensuring data quality	• Intercom has a process that allows data subjects privacy rights (including a right to amend and up Personal Data), as described in Intercom's Privac • See "Measures for ensuring ongoing confidential availability and resilience of processing systems a above.
Measures for ensuring limited data retention	• See "*Measures for ensuring data minimization*" a
Measures for ensuring accountability	• Intercom has implemented data protection polic • Intercom follows a compliance by design approa • Intercom maintains documentation of your proce • Intercom has appointed a data protection officer

	• Intercom adheres to relevant codes of conduct a certification schemes (see "Measures for certific processes and products" above).
Measures for allowing data portability and ensuring erasure	• Secure Disposal. Return or Deletion. Intercom wi and securely delete all live (online or network acc of the Customer Data within 90 days upon Custc deletion request. • Archival Copies. When required by law to retain a Customer Data for tax or similar regulatory purpc Customer Data is stored as a "cold" or offline (i.e immediate or interactive use) backup stored in a facility. • Intercom has a process that allows data subjects privacy rights (including a right to amend and up Personal Data), as described in Intercom's Privac
Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	• Vendor & Services Providers. Prior to engaging n service providers or vendors who will have acces Data, Intercom conducts a risk assessment of ver security practices. • Intercom will restrict the onward sub-processor's Customer Data only to what is strictly necessary Services, and Intercom will prohibit the sub-proc processing the Personal Data for any other purpc • Intercom imposes contractual data protection ob including appropriate technical and organization protect personal data, on any sub-processor it ap require such sub-processor to protect Customer standard required by Applicable Data Protection • Intercom will remain liable and accountable for a DPA that is caused by an act or omission of its su

Schedule 3

LIST OF SUB-PROCESSORS

Annex III

In Clause 9 of the 2021 Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in Section 7.ii (Current Sub-processors and Notification of Sub-processor Changes) of this DPA.

Customer agrees that (a) Intercom may engage Intercom and Sub-processors as listed at https://www.intercom.com/legal/security-third-parties - (the "Sub-processor Page").

Intercom may, by giving reasonable notice to the Customer, add or make changes to the Sub-processor Page. Intercom will notify Customer if it intends to add or replace Sub-processors from the Sub-Processor Page at least 10 days prior to any such changes. In order to receive such notification, Customers can follow link http://privacy.intercom.com/third-party-subscribe to join Intercom's distribution list. If Customer objects to the appointment of an additional Sub-processor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, then Intercom will work in good faith with Customer to find an alternative solution. In the event that the parties are unable to find such a solution, Customer may terminate the Agreement at no additional cost.

Schedule 4

UK Addendum to the EU Commission Standard Contractual Clauses

1. Date of this Addendum: This Addendum is effective from the same date as the DPA.
2. Background: The Information Commissioner considers this Addendum to provide appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.
3. Interpretation of this Schedule 4. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland.

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.
5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.
7. Hierarchy: In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.
8. Incorporation of the Clauses: This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and

b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 7 above, include (without limitation):

a. References to the "Clauses" means this Addendum as it incorporates the Clauses.

b. Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer".

c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.

d. References to Regulation (EU) 2018/1725 are removed.

e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK".

f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner.

g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

h. Clause 18 is replaced to state:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

i. The footnotes to the Clauses do not form part of the Addendum.

10. Amendments to this Addendum

a. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

b. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.

11. Executing this Addendum

a. The Parties may enter into the Addendum (incorporating the Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes (but is not limited to):

i. By attaching this Addendum as Schedule 4 to the Intercom DPA.

ii. By adding this Addendum to the Clauses and including in the following above the signatures in Annex 1A:

"By signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated:" and add the date (where all transfers are under the Addendum)

"By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated" and add the date (where there are transfers both under the Clauses and under the Addendum)

(or words to the same effect) and executing the Clauses; or

iii. By amending the Clauses in accordance with this Addendum and executing those amended Clauses.