STATEMENT OF WORK #1

This Statement of Work (SOW) is governed by the Master Consulting Agreement (the "Agreement") entered into by and between Intercom R&D Unlimited Company("Intercom") and *The Speedshop Ltd Co* ("Service Provider"). This SOW is effective as of the date of last signature below ("SOW Effective Date"). Unless the context requires otherwise, each capitalized term used but not defined herein will have the same definition as in the Agreement. Any conflict between this SOW and the Agreement will be resolved in favor of the Agreement unless specifically stated otherwise herein with reference to the relevant section of the Agreement.

Intercom Point of Contact:
Name: Ryan Sherlock
Address: 124 St Stephens Green, Dublin 2, DC02 C628
Phone: N/A
E-mail: ryan.sherlock@intercom.io

Service Provider Point of Contact:
Name: Nate Berkopec
Address: 1-1-30-1 Hamatake, Chigasaki, Kanagawa, 253-0021 Japan.
Phone: N/A
E-mail: nate.berkopec@speedshop.co

A. Scope of Work

Service Provider will develop and deliver to Intercom the following Services:

Speedshop shall provide education and training services:

- An in-person workshop and training seminar, concerning the topics of Ruby on Rails performance and scalability.

Project Timeline: 5 (Five) consecutive working days between the dates stated below. Dates will be agreed between the parties prior to the start date.

- **Tentative start date:** December 9th, 2024
- **End date:** December 20th, 2024
- **Duration:** 5 days
- 2 days of workshops in 2 locations with 1 non-workshop day in between.

Deliverables:

- All presentation materials, including slides.

Location for Services:

1. December 9th to December 11th in London, address: (to be defined)
2. December 12th to December 20th in Dublin, address: (to be defined)

B. Fee and Payment Schedule

- **Total Charge:** $34,000 USD
- **Deposit:** $10,000 USD upon execution of this agreement
- **Remaining Balance:** Invoiced upon completion of all work
- **Payment Terms:** Invoices will be paid within 30 days of receipt by Client

Intercom will be responsible for additional fees only if the related additions or changes to the scope of work have been agreed to in a writing signed by both parties. If either party gives notice of termination of this SOW as provided in the Agreement, then Service Provider will cease all work under this SOW immediately after such notice has been given and will invoice Intercom for the work done up to the date such notice is given based on a reasonable determination of the percentage completed of each line item of the Project Fees specified above.

C. Estimated Work Schedule

Services will commence on 09 December 2024. The parties estimate in good faith that the project will end on 13 December 2024, unless otherwise extended by mutual written agreement of the parties.

The duly authorized representatives of the parties below have caused this Statement of Work to be executed as of the dates stated below.

Intercom, Inc.		Service Provider:	
By	DocuSigned by: Nikolay Trenin 34557A01E17849F...	By	DocuSigned by: Nate Berkopec 2DD8182315324E3...
Name	Nikolay Trenin	Name	Nate Berkopec
Title	Senior Director, Revenue	Title	Owner
Date	10/18/2024	Date	10/17/2024

STATEMENT OF WORK #2

This Statement of Work (SOW) is governed by the Master Consulting Agreement (the "Agreement") entered into by and between Intercom R&D Unlimited Company("Intercom") and *The Speedshop Ltd Co* ("Service Provider"). This SOW is effective as of the date of last signature below ("SOW Effective Date"). Unless the context requires otherwise, each capitalized term used but not defined herein will have the same definition as in the Agreement. Any conflict between this SOW and the Agreement will be resolved in favor of the Agreement unless specifically stated otherwise herein with reference to the relevant section of the Agreement.

Intercom Point of Contact:
Name: Ryan Sherlock
Address: 124 St Stephens Green, Dublin 2, DC02 C628
Phone: N/A
E-mail: ryan.sherlock@intercom.io

Service Provider Point of Contact:
Name: Nate Berkopec
Address: 1-1-30-1 Hamatake, Chigasaki, Kanagawa, 253-0021 Japan.
Phone: N/A
E-mail: nate.berkopec@speedshop.co

A. Scope of Work
Service Provider will develop and deliver to Intercom the following Services:

Speedshop shall provide consulting services:

- **An in-depth, comprehensive review of the performance and scalability of Intercom's Ruby on Rails application.**
- **Code contributions fixing web application performance issues.**

Project Timeline:

- **Begins: January 1st, 2025**
- **Ends: January 31st, 2025**
- **Duration: 1 month**

Deliverables:

- **Written report**
- **Pull requests and other code contributions**

Work Modality: All work will be performed remotely.

B. Fee and Payment Schedule

- **Total Charge: $20,000 USD**
- **Payment Terms: Invoices will be paid within 30 days of receipt by Client**

Intercom will be responsible for additional fees only if the related additions or changes to the scope of work have been agreed to in a writing signed by both parties. If either party gives notice of termination of this SOW as provided in the Agreement, then Service Provider will cease all work under this SOW immediately after such notice has been given and will invoice Intercom for the work done up to the date such notice is given based on a reasonable determination of the percentage completed of each line item of the Project Fees specified above.

C. Pre-Approved Expenses.

In addition to paying Service Provider the fees described in Section B above, Intercom agrees to reimburse Service Provider for its reasonable out-of-pocket expenses in providing services hereunder, limited to the following: travel expenses for travel completed for the purpose of providing the Services stipulated herein and excluding standard commuter expenses as defined by the U.S. Internal Revenue Service (“I.R.S.”).

D. Estimated Work Schedule

Services will commence on 01 January 2025. The parties estimate in good faith that the project will end on or before 31 January 2025, unless otherwise extended by mutual written agreement of the parties.

The duly authorized representatives of the parties below have caused this Statement of Work to be executed as of the dates stated below.

Intercom, Inc.		Service Provider:	
By	DocuSigned by: Nikolay Trenin 34557A01E17849F...	By	DocuSigned by: Nate Berkopec 2DD8182315324E3...
Name	Nikolay Trenin	Name	Nate Berkopec
Title	Senior Director, Revenue	Title	Owner
Date	10/18/2024	Date	10/17/2024

STATEMENT OF WORK #3

This Statement of Work (SOW) is governed by the Master Consulting Agreement (the "Agreement") entered into by and between Intercom R&D Unlimited Company("Intercom") and *The Speedshop Ltd Co* ("Service Provider"). This SOW is effective as of the date of last signature below ("SOW Effective Date"). Unless the context requires otherwise, each capitalized term used but not defined herein will have the same definition as in the Agreement. Any conflict between this SOW and the Agreement will be resolved in favor of the Agreement unless specifically stated otherwise herein with reference to the relevant section of the Agreement.

Intercom Point of Contact:
Name: Ryan Sherlock
Address: 124 St Stephens Green, Dublin 2, DC02 C628
Phone: N/A
E-mail: ryan.sherlock@intercom.io

Service Provider Point of Contact:
Name: Nate Berkopec
Address: 1-1-30-1 Hamatake, Chigasaki, Kanagawa, 253-0021 Japan.
Phone: N/A
E-mail: nate.berkopec@speedshop.co

A. Scope of Work

Service Provider will develop and deliver to Intercom the following Services:

Speedshop shall provide ongoing consulting services under the following terms:

- **Services Provided: Ongoing support and consultation for Ruby on Rails performance optimization and scalability issues.**
- **Availability: Speedshop will allocate resources to ensure availability for urgent consultations and routine check-ins as agreed upon in the contract terms.**

B. Fee and Payment Schedule

- **Total Charge: $3,000/Monthly**
- **Fee Structure: To be determined based on the agreed scope of services and client needs. Typically, this involves a monthly retainer fee that will be detailed in the contract.**
- **Payment Terms: Invoices will be paid within 30 days of receipt by Client**

Intercom will be responsible for additional fees only if the related additions or changes to the scope of work have been agreed to in a writing signed by both parties. If either party gives notice of termination of this SOW as provided in the Agreement, then Service Provider will cease all work under this SOW immediately after such notice has been given and will invoice Intercom for the work done up to the date such notice is given based on a reasonable determination of the percentage completed of each line item of the Project Fees specified above.

C. Pre-Approved Expenses.

In addition to paying Service Provider the fees described in Section B above, Intercom agrees to reimburse Service Provider for its reasonable out-of-pocket expenses in providing services hereunder, limited to the following: travel expenses for travel completed for the purpose of providing the Services stipulated herein and excluding standard commuter expenses as defined by the U.S. Internal Revenue Service ("I.R.S.").

D. Estimated Work Schedule

Services will commence on 01 January 2025. The parties estimate in good faith that the project will end on or before 31 December 2025. However, the parties agree that Intercom may terminate this SOW for convenience with 30 days prior notice.

The duly authorized representatives of the parties below have caused this Statement of Work to be executed as of the dates stated below.

Intercom, Inc.		Service Provider:	
By	DocuSigned by: Nikolay Trenin 34557A01E17849F...	By	DocuSigned by: Nate Berkopec 2DD8182315324E3...
Name	Nikolay Trenin	Name	Nate Berkopec
Title	Senior Director, Revenue	Title	Owner
Date	10/18/2024	Date	10/17/2024

MASTER CONSULTING AGREEMENT

This Master Consulting Agreement (this "Agreement") is made as of the last date of signature below (the "Effective Date") between Intercom R&D Unlimited Company, located at 124 St Stephen's Green, Dublin 2, D02 C628, Ireland ("Intercom") and *Speedshop* located at *1-1-30-1 Hamatake, Chigasaki, Kanagawa, 253-0021, Japan* ("Service Provider"). The Agreement consists of the terms and conditions set forth below, any attachments or exhibits identified below and any Order Forms or Statements of Work (as defined below) that reference this Agreement.

The following exhibits are incorporated into this Agreement by reference herein:

Exhibit A:	Statement of Work
Exhibit B:	Data Protection Addendum [or RESERVED]
Exhibit C:	Intercom Vendor Security Requirements
Exhibit D:	Consultant Handbook

The parties have caused this Agreement to be duly executed. Each Party warrants and represents that its respective signatories whose signatures appear below are on the date of signature authorized to execute this Agreement.

Intercom R&D Unlimited Company		Service Provider: Speedshop	
By	DocuSigned by: Nikolay Trenin 34557A01E17849F...	By	DocuSigned by: Nate Berkopec 2DD8182315324E3...
Name	Nikolay Trenin	Name	Nate Berkopec
Title	Senior Director, Revenue	Title	Owner
Date	10/18/2024	Date	10/17/2024

1. DEFINITIONS

"Services" means the work to be performed by Service Provider for, or on behalf of Intercom, pursuant to this Agreement and described in a Statement of Work.

"Statement of Work" or **"SOW"** means a mutually-executed written description of the Services and any work product or deliverables to be provided. SOWs shall contain a reference to this Agreement by its name and date, applicable fees and payment schedule, and the date the Services will start and are scheduled to end. A template of an SOW is attached hereto as **Exhibit A**. Each SOW shall by reference incorporate the terms and conditions of this Agreement. This Agreement shall govern each SOW and unless expressly set forth in an SOW, this Agreement shall take precedence over any conflicting or inconsistent terms in an SOW. SOWs supersede any and all proposals provided by Service Provider to Intercom relating to any of the work described in the SOW; however, Service Provider represents and warrants to Intercom that any and all statements and representations regarding Service Provider and Service Provider's services and capabilities made in such proposals are true and correct.

“Security Incident” means any unauthorized access or breach of security leading to, or reasonably believed to have led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data.

“Personal Data” means information provided by Intercom under this Agreement relating directly or indirectly to an identified or identifiable natural person (“data subject”), including but not limited to a name, email address, identification number, location data, or online identifiers, etc.

2. PERFORMANCE STANDARDS.

Unless otherwise specified in an SOW, Service Provider shall be solely responsible for determining the method, details and means of performing the Services. Service Provider shall provide the Services personally, and may not assign or subcontract the provision of the Services to any other person, firm or company without the prior written consent of Intercom. Service Provider will provide information regarding performance of the Services upon request, including, among other things, progress and other operational reports, and an opportunity to inspect and review work in progress. If Service Provider performs any Services at Intercom’s offices or at any of Intercom’s customers’ facilities, Service Provider will comply with all applicable security, safety, and health policies and procedures.

3. PAYMENT

3.1 Fees. Except to the extent provided otherwise in the applicable SOW, Service Provider will invoice Intercom monthly in arrears for such fees as agreed in such SOW or Order Form. An SOW may estimate fees only to the extent that Services will be billed on a time-and-materials basis, in which case Service Provider agrees it will not invoice or otherwise charge Intercom more than estimated for any line item unless Intercom has pre-approved in writing and the estimate for that line item specifies how the actual fee will be calculated. Each invoice will explain how all fees have been determined and will include such other information as Intercom may specify from time to time.

3.2 Expenses. All expenses incurred by Service Provider in performing the Services will be borne by Service Provider, unless otherwise pre-approved by Intercom in writing. Service Provider will submit in arrears expense reports with receipts and any other documentation that Intercom may reasonably request.

3.3 Invoicing. Each proper undisputed invoice and expense report submitted to Intercom will be due and payable forty-five (45) days from the date of receipt of valid invoice. On termination of an SOW for any reason permitted by this Agreement, Intercom will pay Service Provider a proportionate value of the Services completed as of the effective date of such termination provided that Service Provider has delivered to Intercom the portion of the Services completed. All amounts payable under this Agreement will be paid in U.S. dollars less any required government withholding, including but not limited to applicable sales, use and similar taxes. Intercom will not be responsible for paying any tax not specified on an SOW and the corresponding invoice.

4. WORKING RELATIONSHIP AND RIGHTS OR OWNERSHIP

4.1 No Agency. Intercom and Service Provider are independent contractors and neither party is the legal representative, agent, joint venturer, partner, employee or employer of the other party for any purpose whatsoever, and neither party has any right, power or authority to assume or create any obligation of any kind or to make any representation or warranty on behalf of the other party, whether express or implied, or to bind the other party in any respect.

4.2 No Benefits or Contributions. Neither Service Provider nor Service Provider's employees, agents or representatives are entitled to any of the benefits that Intercom may make available to its own employees, such as group insurance, profit sharing or retirement benefits. Service Provider will be solely responsible for, and will file on a timely basis, all tax returns and payments required to be filed with or made to any federal, state or local tax authority with respect to Service Provider's performance of the Services and receipt of compensation under this Agreement. Service Provider shall have the full responsibility for compliance with all applicable laws, rules and regulations applicable to the Services, all applicable labor and employment requirements with respect to Service Provider's Assigned Personnel, its designation of self-employment, sole proprietorship or other form of business organization, and with respect to the personnel, including jurisdictionally required insurance coverage (i.e., workers compensation) and any jurisdictional immigration or work visa requirements.

4.3 Assigned Personnel. If Service Provider assigns any of its employees, Service Providers, contractors or other personnel (the "Assigned Personnel") to perform any of the Services at Intercom's offices or facilities (other than occasional visits for meetings with Intercom that are not scheduled on a regular basis), then in compliance with and to the extent permitted by applicable laws: (i) Service Provider will ensure that each Assigned Personnel has properly demonstrated eligibility to work in the jurisdiction in which the Services will be performed; (ii) Service Provider will, in accordance with applicable law, conduct a criminal background check on each Assigned Personnel covering the counties, states, and/or countries in which such person was employed or resided for the past seven years and in such other areas as Intercom may reasonably specify (such as a driving record check, credit check, etc.); (iv) Service Provider will not provide any Assigned Personnel who: (a) has any felony convictions or misdemeanor convictions involving violence or dishonesty; (b) has a restriction (e.g.. a court order or restrictive covenant) that would prevent the person from providing services or impose limitations on the services that the person is able to provide to Intercom; (c) may present a higher than normal security risk to Intercom; or (d) does not meet other guidelines specified by Intercom from time to time. Intercom may at any time request that Service Provider remove an Assigned Personnel and Service Provider shall comply with such request as soon as possible.

4.4 Intercom Facilities and Equipment. If any Service Provider personnel visits or performs Services at any Intercom office or facility, then Service Provider will ensure that such personnel complies with all applicable Intercom rules and policies and other requests from Intercom and takes all necessary precautions to prevent injury to any person or damage to any property. Service Provider shall indemnify, defend and hold Intercom harmless for any breach or alleged breach of this Section 4.4.

4.5 Pre-Existing Property and Ownership. All Services are "works for hire" and any and all work product, deliverables, code, data, information or reports that are referenced in any SOW or otherwise provided to Intercom as part and parcel of this Agreement is and shall be the sole and exclusive property of Intercom and shall be deemed to be Intercom intellectual property and subject to all non-disclosure and other protections afforded hereunder. Service Provider hereby assigns to Intercom any and all rights it may obtain to any such work product or deliverable. Service Provider shall execute any and all documentation as may be required to effectuate the requirements of this section 4.5. Intercom owns all of its data, customer and employee information, and all information regarding its technology and its business, and this Agreement effectuates no license or transfer of any such Intercom information or materials to Service Provider or other third party. Service Provider owns and continues to own any Service Provider developed data, information or technology that pre-exists this Agreement less any Intercom intellectual property that may be contained therein. However, Service Provider hereby grants to Intercom a fully paid, royalty free, perpetual, non-terminable and global license to use any such Service Provider data, information or technology for any legitimate Intercom business purpose related to the Services.

5. REPRESENTATIONS AND WARRANTIES

5.1 By Intercom. Intercom warrants to Service Provider that Intercom is duly organized, validly existing and in good standing under the laws of the jurisdiction of its organization, that this Agreement has been duly authorized by all necessary corporate action, and that this Agreement is the legal, valid, and binding obligation of Intercom, enforceable against Intercom in accordance with its terms.

5.2 By Service Provider. Service Provider represents and warrants to Intercom that:

5.2.1 Service Provider is duly organized, validly existing and in good standing under the laws of the jurisdiction of its organization, that this Agreement has been duly authorized by all necessary corporate (or other entity) action, and that this Agreement is the legal, valid, and binding obligation of Service Provider, enforceable against Service Provider in accordance with its terms.

5.2.2 Service Provider has obtained any and all consents, permits, licenses and authorizations necessary for or in connection with providing the Services to Intercom. Service Provider’s entry into or performance of this Agreement does not and will not violate any other agreement by which Service Provider is bound, and Service Provider has full power, authority, unrestricted ability and all rights (including but not limited to license rights of intellectual property) necessary: to enter into this Agreement; and to perform all of Service Provider's obligations hereunder.

5.2.3 The Services will be performed by qualified personnel in a timely, workmanlike, and best-efforts manner and will meet and conform to all specifications as stated in any applicable SOW. The Services and any work product and/or deliverable shall be of the highest prevailing standard within Service Provider’s industry, and shall meet the reasonable requirements of Intercom as stated within any SOW. In the event of a breach of this warranty, Intercom shall notify Service Provider in writing as the specifications of any such breach, whereupon Service Provider shall, at the reasonable discretion of Intercom, re-perform all non-conforming services at no additional charge to Intercom, replace any non-conforming work product or deliverable with a fully conforming item or deliverable, or refund any and all applicable fees paid for any such non-conforming work product or deliverable. Service Provider shall be liable for any and all reasonable costs of cover and\or replacement Services in the event of a breach of these warranties.

5.2.4 Service Provider and its employees, and contractors have complied and will comply with all laws, rules, regulations and ordinances applicable to the provision of the Services.

5.2.5 Service Provider and its employees, and contractors will comply with Intercom’s Partner Code of Conduct at: https://www.intercom.com/legal/partner-code-of-conduct .

6. INSURANCE

Service Provider will (at Service Provider's sole cost and expense) obtain and maintain all appropriate insurance coverages required by federal or state law (including without limitation workers' compensation and disability insurance). Service Provider will also (at Service Provider's sole cost and expense) maintain the following minimum insurance coverages during the term of the Agreement: (a) comprehensive general liability insurance for bodily injury, death, and property damage with a per occurrence limit of at least $1,000,000, with such policy to include broad-form contractual liability, advertisers liability, protective liability, and personal injury/property damage coverage; (b) workers' compensation and employer's liability coverage of at least $1,000,000; (c) comprehensive automobile liability insurance for all owned, leased, non-owned, and hired vehicles with policy limits of at least $1,000,000 combined single limit for bodily injury and property damage; (d) if any of Service Provider's personnel are to visit or perform Services at any of Intercom’s offices or facilities, then fidelity bond coverage (or an employee crime policy) of at least $1,000,000; and (e) if Service Provider will have any access to any personally identifiable information of Intercom users or Service Provider provides computer programming services to Intercom, then Professional Liability Insurance (Errors & Omissions) in the amount of at least $5,000,000 for each claim covering the products and/or services provided by Service Provider. The Professional Liability Insurance policy (if required) will not exclude claims based on computer virus, computer attack, e-commerce transactions, or breach of security. Each insurance policy required by this Section will be with an insurance company rated at least A-, VII by the most recent AM Best ratings guide. The fact that this Section requires Service Provider to maintain insurance with certain minimum coverages will not be deemed to limit Service Provider’s liability under this Agreement in any way.

7. INDEMNIFICATION

Service Provider will defend, indemnify, and hold harmless Intercom its subsidiaries and affiliates, and their respective directors, officers, employees and agents (collectively, the “Indemnified Parties”), against and from any and all claims, losses, liabilities, damages, suits, actions, government procedures, taxes, penalties or interest, (including reasonable attorneys’ fees and costs of suit) that may be imposed on, incurred by, or asserted against any Indemnified Parties resulting from, arising out of, or relating to any third party claims for the following: (a) the performance of the Services or Service Provider's obligations under this Agreement by Service Provider (or any of Service Provider's employees, Assigned Personnel, Service Providers, contractors, or agents); (b) any claim that any part of the Services, the Deliverables, the Invention, or the use thereof: (i) infringes any patent, copyright, trademark right, or other Intellectual Property Right of a third party, (ii) is a misappropriation of any third party trade secret, or (iii) violates any other rights of a third party; (c) security incidents and/or breaches of applicable privacy laws; and (d) any claims arising from a death, bodily injury, tortious conduct or damage to real or personal property, provided, however, that Service Provider shall not be required to indemnify or hold harmless Intercom to the extent that claims and or costs arise out of the gross negligence or willful misconduct of Intercom or its employees. Service Provider will not enter into any settlement that affects Intercom’s rights or interest without Intercom’s prior written approval. Intercom will have the right to participate in the defense of any applicable claim at Intercom’s own expense. In the event of a violation of this Section (i), Service Provider shall, at the reasonable discretion of Intercom, procure at Service Provider’s expense and for the benefit of Intercom a license to use the allegedly infringing item, or replace the applicable deliverable or work product with a non-infringing item with the same or better features and/or functionality or refund any and all applicable fees paid by Intercom. These remedies are in addition to and independent of the indemnification obligations listed herein.

8. LIMITATION OF LIABILITY

EXCEPT WITH RESPECT TO A VIOLATION OF INTERCOM’S RIGHTS IN ITS INTELLECTUAL PROPERTY, A BREACH OF ANY PRIVACY OR SECURITY OBLIGATION IMPOSED BY THIS AGREEMENT, BREACHES OR OBLIGATIONS OF **SECTION 5 (REPRESENTATIONS AND WARRANTIES), SECTION 9 (CONFIDENTIAL INFORMATION AND PERSONAL DATA), OR INDEMNIFICATION OBLIGATIONS IN THIS AGREEMENT,** NEITHER PARTY WILL BE LIABLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOST PROFITS (HOWEVER ARISING, INCLUDING NEGLIGENCE) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL INTERCOM BE LIABLE TO SERVICE PROVIDER FOR AN AMOUNT GREATER THAN THE AMOUNTS PAID OR PAYABLE BY INTERCOM HEREUNDER.

9. CONFIDENTIAL INFORMATION AND PERSONAL DATA

9.1 Confidentiality Obligations. Service Provider agrees to hold the Confidential Information of Intercom in strict confidence and agrees not to disclose any Confidential Information to any third party. Confidential Information includes, but is not limited to, this Agreement, product roadmap, software, product and technology-related information, customer lists, financial information, sales, marketing, non-public company information and activities, and business plans. Service Provider will have no right, title or interest in Confidential Information obtained by it under this Agreement. Upon termination of this Agreement or SOW for any reason, Service Provider will promptly contact Intercom for instructions and will follow such reasonable instructions by Intercom regarding the return, destruction or other appropriate action with regard to Confidential Information. This Section 9 supplements but does not replace any existing non-disclosure agreement by the parties, which is hereby incorporated by reference.

9.2. Data Protection. Under this Agreement, Service Provider may obtain from Intercom certain information relating to identified or identifiable individuals ("Personal Data"). The Data Processing Addendum ("DPA") attached hereto as Exhibit B will govern Service Provider's access to Personal Data. In the event Service Provider acquires access to Personal Data without having first executed a DPA with Intercom, the parties hereby agree and incorporate by reference 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 and the related Data Security Requirements as defined in this Section 9.2 and 9.3. Upon execution of the DPA, in the event of a conflict between 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 and the DPA, the DPA will control. Service Provider represents and warrants that it will only use the Personal Data from Intercom for the provision of Services under this Agreement or the applicable SOW and will not share, transfer, or otherwise use the Personal Data for any other purpose.

9.3 Data Protection Compliance Cooperation. In the event of an investigation by a data protection regulator or similar authority regarding Personal Data, Service Provider will provide Intercom with reasonable assistance and support, including, where necessary, access to Service Provider's premises to the extent needed to respond to such investigation. In the event that Service Provider is unable to comply with the obligations stated in this Agreement, Service Provider will promptly notify Intercom, engage a third party audit services provider at Service Provider's cost to retrieve any needed information or complete any required compliance actions for Intercom, and Intercom may do one or more of the following: (a) suspend the transfer of Personal Data to Service Provider; (b) require Service Provider to cease processing Personal Data; (c) demand the return or destruction of Personal Data; or (d) immediately terminate this Agreement or any applicable SOW.

10. COMPLIANCE SECURITY REQUIREMENTS

As applicable, Service Provider will comply with the Intercom Vendor Security Requirements, attached hereto as Exhibit C and shall provide to Intercom all reasonably required information in order for Intercom to ensure compliance therewith. Additionally, Service Provider agrees that Service Provider and its employees and contractors will abide by Intercom's Partner Code of Conduct attached hereto as Exhibit D and our acceptable use polices and behavioral standards ("Consultant Handbook") attached hereto as Exhibit D.

11. TERM AND TERMINATION

11.1 Term. This Agreement will take effect on the Effective Date and will continue in effect for three (3) years (the "Term") unless terminated earlier in accordance with this Agreement.

11.2 Termination for Convenience. Intercom may terminate this Agreement or any SOW at any time by giving to Service Provider written notice of termination thereof at least thirty (30) days prior to the date of termination, except that Intercom may terminate any SOW with at least fifteen (15) days notice prior to the date Services stipulated in the SOW are scheduled to commence with no obligation to reimburse Service Provider for out-of-pocket expenses related to scheduling such Services. Termination of the Agreement will also serve to terminate any SOW in progress. Service Provider may terminate the Agreement at any time that there is no uncompleted SOW in effect by giving to Intercom written notice of termination thereof at least thirty (30) days prior to the date of termination.

11.3 Termination for Cause. Intercom is entitled to terminate this Agreement by providing notice to Service Provider, if Service Provider: (i) commits a serious breach of any obligations owed to Intercom under this agreement, and in Intercom's commercially reasonable judgment, is unable to immediately cure such breach; (ii) fails, or continues to fail, or refuses to provide the Services to the standards or time scales reasonably required by Intercom.

11.4. Return of Materials. When this Agreement expires or is terminated, Service Provider shall promptly return any Confidential Information and Personal Data in Service Provider's possession to Intercom pursuant to Section 9, Confidential Information and Personal Data.

12. GENERAL PROVISIONS

12.1 No Publicity. Except to the extent that Service Provider obtains the prior written approval of Intercom, Service Provider will not directly or indirectly issue or permit the issuance of any publicity, press or news release, or other public statement concerning the relationship between the parties, this Agreement, any SOW, the terms hereof or thereof, or any of the transactions contemplated hereby or thereby; and will not use the name, trademarks, or service marks of Intercom in any promotional materials.

12.2 Force Majeure. Neither party shall be liable to the other for delayed performance caused by events outside of its reasonable control, including war, civil unrest, fire, earthquake or other natural disaster, provided that the party affected by such force majeure provides prompt notice of it to the other party and uses reasonable efforts to overcome its effects.

12.3 Assignment. Service Provider may not assign this Agreement or Service Provider's rights, nor delegate Service Provider's duties hereunder, without Intercom's prior written consent.

12.4 Entire Agreement. This Agreement (including the Attachments hereto which are incorporated herein by this reference) and any other documents expressly contemplated hereby constitute the entire agreement between the parties with respect to the subject matter hereof.

12.5 Severability. If any provision of this Agreement is for any reason held to be invalid, illegal, or unenforceable under applicable law in any respect, then this Agreement will be construed as if such invalid, illegal, or unenforceable provision were excluded from this Agreement.

12.6 Waiver. No waiver of any provision of this Agreement will be effective unless in writing and signed by the party against whom such waiver is sought to be enforced.

12.7 Amendment. This Agreement may only be amended, modified, or supplemented by an instrument in writing specifically mentioning this Agreement and signed by the party against whom such amendment, modification, or supplement is sought to be enforced.

12.8 Notices. Any notice, demand, request, or other communication required or permitted to be given under this Agreement (any "Notice") will be made in writing and will be delivered by personal delivery (with notice deemed given when delivered personally), by overnight courier (with notice deemed given upon written verification of receipt), by certified or registered mail, return receipt requested (with notice deemed given upon verification of receipt), or by electronic mail (also "email") (with notice deemed given upon receipt of email). Notices will be addressed to a party as provided in this Section or such other address as such party may request by notifying the other party (or parties) thereof in writing. Any notice sent to Intercom via email must be sent to "legal@intercom.io." Any notice to Service Provider will be addressed to the address indicated as such on the signature page hereto.

12.9 Specific Performance; Remedies Cumulative. Each Party acknowledges that a breach of this Agreement cannot be adequately compensated for by money damages. Each Party acknowledges that compliance with the provisions of this Agreement is necessary in order to protect the proprietary rights of each Party. Each Party further acknowledges that any unauthorized use or disclosure to any third party in breach of this Agreement will result in irreparable and continuing damage to the other Party. Accordingly, each Party hereby consents to the issuance of any injunctive relief or the enforcement of other equitable remedies against it at the suit of the injured Party (without bond or other security), to compel performance of any of the terms of this Agreement, and waives any defenses thereto, including without limitation the defenses of failure of consideration, breach of any other provision of this Agreement, and availability of relief in damages. All remedies, whether under this Agreement, provided by law, or otherwise, shall be cumulative and not alternative.

12.10 Governing Law and Venue. This Agreement will be governed by the laws of the State of California, without regard to its choice of law provisions. Each of the parties hereto consents to the exclusive jurisdiction and venue of the state and federal courts of San Francisco, California.

EXHIBIT A

STATEMENT OF WORK # ___

This Statement of Work (SOW) is governed by the Master Consulting Agreement (the "Agreement") entered into by and between [Intercom, Inc. or Intercom R&D Unlimited Company] ("Intercom") and __________ ("Service Provider"). This SOW is effective as of the date of last signature below ("SOW Effective Date"). Unless the context requires otherwise, each capitalized term used but not defined herein will have the same definition as in the Agreement. Any conflict between this SOW and the Agreement will be resolved in favor of the Agreement unless specifically stated otherwise herein with reference to the relevant section of the Agreement.

Intercom Point of Contact:
Name:
Address:
Phone:
E-mail:

Service Provider Point of Contact:
Name:
Address:
Phone:
E-mail:

A. Scope of Work

Service Provider will develop and deliver to Intercom the following Services:

[TO BE INSERTED HERE]

B. Fee and Payment Schedule

[TO BE INSERTED HERE]

Intercom will be responsible for additional fees only if the related additions or changes to the scope of work have been agreed to in a writing signed by both parties. If either party gives notice of termination of this SOW as provided in the Agreement, then Service Provider will cease all work under this SOW immediately after such notice has been given and will invoice Intercom for the work done up to the date such notice is given based on a reasonable determination of the percentage completed of each line item of the Project Fees specified above.

C. Pre-Approved Expenses.

In addition to paying Service Provider the fees described in Section B above, Intercom agrees to reimburse Service Provider for its reasonable out-of-pocket expenses in providing services hereunder, limited to the following: travel expenses for travel completed for the purpose of providing the Services stipulated herein and excluding standard commuter expenses as defined by the U.S. Internal Revenue Service ("I.R.S.").

D. Estimated Work Schedule

Services will commence on __________________, 20__. The parties estimate in good faith that the project will end on _________________, 20__, unless otherwise extended by mutual written agreement of the parties.

The duly authorized representatives of the parties below have caused this Statement of Work to be executed as of the dates stated below.

Intercom R&D Unlimited Company		Service Provider:	
By		By	
Name		Name	
Title		Title	
Date		Date	

EXHIBIT B

DATA PROCESSING ADDENDUM

This DPA forms part of the Agreement and sets out the terms that apply when Personal Data is processed by Vendor as a Processor or Subprocessor (where applicable) on behalf of Intercom under the Agreement. The purpose of this DPA is to ensure such processing is conducted in accordance with Applicable Data Protection Legislation and contractual obligations. Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement. Nothing in this DPA relieves Vendor of its own direct responsibilities under Applicable Data Protection Legislation.

1. Definitions

For the purposes of this DPA:

(a) "**Applicable Data Protection Legislation**" refers to laws and regulations applicable to Vendor'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 2018 ("**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**"), and (d) CCPA, in each case, as may be amended, superseded or replaced.

(b) "**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.

(c) "**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. It shall have the same meaning ascribed to "controller" under the GDPR and other equivalent terms under Applicable Data Protection Legislation (e.g., "business" as defined under the CCPA), as applicable.

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

(e) "**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).

(f) "**Personal Data**" or "personal data" or "personal information" 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.

(g) "**Processor**" or "**processor**" means the entity which processes Personal Data on behalf of the Controller. It shall have the meaning ascribed to "processor" under the GDPR and other equivalent terms under other Applicable Data Protection Legislation (e.g., "service provider" as defined under the CCPA), as applicable.

(h) "**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.

(i) "**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.

(j) "**Security Breach**" means a breach of security leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, alteration, or access to Personal Data transmitted, stored or otherwise processed by Vendor. A Security Breach shall not include an unsuccessful attempt or activity that does not compromise the security of Personal 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.

(k) "**Services**" means the services described in the Agreement between the parties;

(l) "**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).

(m) "**Subprocessor**" or "**Sub-processor**" means any processor appointed by Processor to process Personal Data on behalf of Intercom.

(n) "**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 of DPA

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

2.2 **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.

3. Roles and Responsibilities

3.1 **Parties' Roles.** To the extent that Vendor processes Personal Data on behalf of Intercom subject to Applicable Data Protection Legislation in the course of providing the Services, it will do so only as a Processor acting on behalf of Intercom and in accordance with the requirements of the Agreement.

3.2 **Instructions**. Vendor shall process Personal Data only for the purposes of performing its obligations under this DPA and the Agreement, and in accordance with the instructions of Intercom from time to time.

i. ersonal Data such as account data, Intercom is a controller and Vendor is an independent controller, not a joint controller with Intercom. Vendor will process such data as a controller (a) in order to manage the relationship with Intercom; (b) carry out Vendor’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 Vendor’s legal or regulatory obligations; and (f) as otherwise permitted under Applicable Data Protection Legislation and in accordance with this DPA, and the Agreement.

3.3 **Purpose Limitation**. Vendor 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.

3.4 **Obligations**. Vendor shall at all times comply with its obligations as a Processor under the Applicable Data Protection Legislation and its obligations in respect of Personal Data under this DPA, and it will not do, or permit anything to be done, which might cause Intercom to be in breach of the Applicable Data Protection Legislation. Vendor shall also promptly notify Intercom prior to carrying out any instruction from Intercom if, in Vendor's opinion, such instruction is likely to result in processing that is in breach of the Applicable Data Protection Legislation.

4. Security

4.1 Vendor will have in place and maintain throughout the term of this DPA appropriate technical and organizational measures designed to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing (e.g., a Security Breach) including, without limitation and at a minimum, the technical and operational measures identified in Schedule 2 (Technical and Organizational Security Measures).

4.2 Vendor shall ensure that any person that it authorizes to process the Personal Data (including its staff, agents, representatives, advisors and subcontractors) shall be informed of the confidential nature of the Personal Data and are subject to a duty of confidentiality (whether a contractual or a statutory duty) which shall continue to apply following the conclusion of the Services.

4.3 Upon becoming aware of a Security Breach, Vendor shall notify Intercom without undue delay (and in any event within forty-eight (48) hours) and shall, at no additional charge, provide all such information as Intercom may require, including to enable Intercom to fulfill its data breach reporting obligations under Applicable Data Protection Legislation. Vendor will remedy each Security Breach in a timely manner and provide Intercom written details regarding Vendor's internal investigation regarding each Security Breach. Vendor will cooperate and work together with Intercom to formulate and execute a plan to rectify all confirmed Security Breaches. Vendor shall not communicate with any data subjects, supervisory authorities or other parties in respect of the Security Breach without the prior written consent of Intercom.

4.4 **Human Resources Security**.

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

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

4.5 Upon request by Intercom, Vendor shall fully and promptly cooperate with Intercom and take all steps as are directed by Intercom to assist in the investigation, mitigation and remediation of each Security Breach, in order to enable Intercom to (i) perform a thorough investigation into the Security Breach, (ii) formulate a correct response and (iii) to take suitable further steps in respect of the Security Breach in order to meet any requirement under the Applicable Data Protection Legislation.

5. Subprocessing

5.1 Where Vendor seeks to appoint a Subprocessor, Vendor shall notify Intercom by email at dataprotection@intercom.com indicating the name, country location, and subcontracted service of the proposed new Subprocessor. Intercom shall have thirty (30) days to object to the appointment of the Subprocessor. If Intercom does not object, Vendor may use the new

Subprocessor for the indicated data processing activities. If Intercom objects within the given timeline, Vendor will use reasonable efforts to change the Services to avoid processing of the Personal Data by the proposed Subprocessor, the subject of the objection. If Vendor is unable to implement such changes within a reasonable period of time, which shall not exceed thirty (30) days from receipt of Intercom's written objection, Intercom may, without penalty, terminate the Services, or, on its election, the provision of the affected Services on notice to the Vendor.

5.2 Vendor shall ensure that each Subprocessor appointed in accordance with this DPA enters into a written contract with Vendor which provides for data protection obligations that protect the Personal Data to the same extent provided for by this DPA.

5.3 Vendor shall remain liable for breach of the DPA and/or Applicable Data Protection Legislation caused by a Subprocessor. Vendor shall promptly make available to Intercom a list of Subprocessors on request.

6. International Transfers

6.1 Vendor will at all times provide an adequate level of protection for the Personal Data (and ensure that any further Subprocessors (including any affiliates) do the same), wherever processed, in accordance with the requirements of Applicable Data Protection Legislation and this DPA.

6.2 safeguard under Article 46 GDPR for transfers to the United States, then the parties agree that when the transfer of personal data from Intercom (as "data exporter") to Vendor (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:

i. In relation to transfers of Personal Data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:
   a. Module Two or Module Three will apply (as applicable);
   b. in Clause 7, the optional docking clause will apply;
   c. 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 5.1 of this DPA;
   d. in Clause 11, the optional language will not apply;
   e. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the EU Member State in which the data exporter is established and if no such law, by Irish law;
   f. 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;
   g. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and
   h. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA;

ii. In relation to transfers of Personal Data protected by the GDPR and processed in accordance with Section 3.2.i. of this DPA, the EU SCCs shall apply, completed as follows:

a. Module One will apply;
b. in Clause 7, the optional docking clause will apply;
c. in Clause 11, the optional language will not apply;
d. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
e. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
f. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and
g. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA;

iii. 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:

a. references to "Regulation (EU) 2016/679" shall be interpreted as references to UK Privacy Laws or the Swiss DPA (as applicable);
b. 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);
c. 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);
d. 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);
e. 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);
f. 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);
g. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and
h. 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.

iv. To the extent that and for so long as the EU SCCs as implemented in accordance with sub-paragraph (i)-(iii) above cannot be used to lawfully transfer Personal 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.

a. In relation to data that is protected by the UK GDPR, the EU SCCs will apply as follows: (i) 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".

v. to the extent of such conflict.

6.3 Alternative Transfer Mechanism. To the extent that Vendor adopts an alternative data export mechanism (including any new version of or successor to the DPF or Standard Contractual Clauses adopted pursuant to Applicable Data Protection Legislation) ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall upon notice to Intercom 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 Personal Data is transferred).

6.4 The parties agree that if the DPF or Standard Contractual Clauses are replaced, amended or no longer recognized as valid under Applicable Data Protection Legislation, or if a Supervisory Authority and/or Applicable Data Protection Legislation requires Intercom or its affiliates to adopt an alternative transfer solution, Vendor will: (i) promptly take such steps requested by Intercom including putting an alternative transfer mechanism in place to ensure the processing continues to comply with Applicable Data Protection Legislation; or (ii) cease the transfer of Personal Data and at Intercom's option, delete or return the Personal Data to Intercom.

7. Cooperation

7.1 Vendor shall assist Intercom with data protection impact assessments or consultations with Supervisory Authorities in relation to Personal Data.

8. Audit

8.1 Vendor shall, at no cost to Intercom, allow for and contribute to audits and make available to Intercom all information necessary, including inspections, conducted by Intercom or another auditor mandated by Intercom for the purpose of demonstrating compliance by Intercom with its obligations under this Agreement and compliance with Applicable Data Protection Legislation.

9. Data Subjects' Rights

9.1 Vendor shall promptly inform Intercom by email at dataprotection@intercom.com if it receives a request or complaint from a data subject.

9.2 Vendor shall assist Intercom to enable Intercom (or its third-party Controller) to respond to any requests, complaints or other communications from data subjects and regulatory or judicial bodies relating to the processing of Personal Data under the Agreement, including requests from data subjects seeking to exercise their rights under Applicable Privacy Laws. All responsive materials to requests made by Intercom must be provided to Intercom within twenty (20) days of the request if the request was prompted as a result of either a request from a (1) data subject right request ("SAR") or (2) governmental authority. In the event that any such request, complaint or communication is made directly to Vendor, Vendor shall promptly pass this onto Intercom, no later than three (3) business days after receipt, and shall not respond to such communication without Intercom's express authorization.

10. Deletion / Return of Personal Data.

10.1 Upon termination or expiry of the Agreement, Vendor shall, at the choice of Intercom, immediately delete or return to Intercom all Personal Data (including copies) in Vendor's possession or control, as soon as reasonably practicable and within a maximum period of thirty (30) days' of termination or expiry of the Agreement, unless and only to the extent that Vendor is required by any applicable European or EEA member state law, (or in the case of personal data the processing of which is subject to UK data protection law, applicable UK law) to retain some or all of the Personal Data and then only for that limited purpose. Vendor shall confirm, on request, in writing that any deletion or return has taken place.

11. CCPA

11.1 For purposes of this Section 11, the terms "business," "commercial purpose," "sell" and "service provider" have the meanings given in the CCPA, and "personal information" shall mean Personal Data that constitutes "personal information" governed by the CCPA.

11.2 It is the parties' intent that with respect to any personal information, Intercom is a business and Vendor is a service provider. Vendor shall not (a) sell any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Services; or (c) retain, use or disclose the personal information outside of the direct business relationship between the parties. Vendor hereby certifies that it understands its obligations under this Section 11 and will comply with them.

11.3 The parties acknowledge and agree that Vendor's provision of the Services encompasses, and that the parties' business relationship contemplates, Vendor's performance of its obligations and exercise of its rights under the Agreement.

12. Miscellaneous

12.1 This DPA contains certain terms required by Intercom relating to data protection, privacy and security which has been updated to reflect certain requirements of the GDPR and the CCPA, where applicable. In the event (and to the extent only) of a conflict (whether actual or perceived) between the GDPR and the CCPA, 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.

12.2 Vendor shall share with Vendor's staff and/or subcontractor (where applicable), the terms of Intercom's Privacy Policy which has been provided and may be amended from time to time, which details how Personal Data (as applicable) will be processed by Intercom.

12.3 Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 3.1 and 3.2.i., Intercom reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation.

12.4 If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail to the extent of the conflict.

12.5 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

12.6 Notwithstanding anything in the Agreement or any statement of work, order form or purchase order entered in connection therewith, the parties acknowledge and agree that Vendor's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

Schedule 1

DETAILS OF PROCESSING

Annex I

A. LIST OF PARTIES

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

Name of Data Importer:	The party identified as the "Vendor" 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 DPA is executed by Vendor.
Role (controller/processor):	Processor

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:	Intercom, Inc.
Address:	55 2nd Street, 4th Floor San Francisco, CA 94105 USA
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 DPA is executed by Intercom.
Role (controller/processor):	Controller or Processor

B. DESCRIPTION OF PROCESSING/ TRANSFER

Categories of Data Subjects whose personal data is transferred	**Module One** Intercom's employees and individuals authorized by Intercom to access Intercom's account: Employees or contact persons of Intercom's prospects, customers, business partners and vendors.

	Modules Two and Three Intercom's end users: Prospects, customers, business partners and vendors of Intercom (who are natural persons).
Categories of Personal Data transferred	**Module One** Data which constitutes Personal Data, such as name and contact information as well as Intercom billing address(es).
	Modules Two and Three Any Personal Data processed by Vendor 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 ● Identification and contact data (name, title, address, phone number, email address); ● Financial information (credit card details, account details, payment information); ● Employment details (employer, job title, academic and professional qualifications, geographic location, area of responsibility, affiliated organization, area of responsibility, health data, and industry); ● IT related data (IP addresses of visitors to Intercom's customer's websites, online navigation data, browser type, language preferences, pixel data, cookies data, web beacon data); ● ID connection, location, family, history data; ● IT information (computer ID, user ID and password, domain name, IP address, log files, software and hardware inventory, software usage pattern tracking information (i.e. cookies and information recorded for operation and training purposes).
Sensitive data transferred (if applicable) and applied restrictions or safeguards	*The personal data transferred may include the following special categories of data:* (Insert if applicable)
Frequency of Transfer	Continuous.
Nature and purpose(s) of the data transfer and Processing	**Module One** Personal data processed to manage the account, including to access Intercom'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 will be subject to the following basic processing activities: Vendor will process personal data as necessary to provide the Services under the Agreement. Vendor does not sell Intercom's Personal Data or Intercom's 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.
Retention period (or, if not possible to determine, the criterial used to deter- mine the period)	**Module One** Vendor will process Personal Data as long as required (a) to provide the Services to Intercom; (b) for Vendor's lawful and legitimate business needs; or (c) in accordance with applicable law or regulation.
	Modules Two and Three Upon termination or expiry of this Agreement, Vendor will delete or return to Intercom all Personal 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 Vendor is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data Vendor 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** Vendor will restrict the onward sub-processor's access to Personal Data only to what is strictly necessary to provide the Services, and Vendor will prohibit the sub-processor from processing the Personal Data for any other purpose. Vendor 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 Personal Data to the standard required by Applicable Data Protection Legislation.

	Vendor will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its subprocessors.
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

Where applicable, this Schedule 2 will serve as Annex II to the Standard Contractual Clauses. The following table attached hereto as **Exhibit C: Intercom Vendor Security Requirements** provides more information regarding the technical and organizational security measures set forth therein.

Description of the technical and organisational measures implemented by the Processor(s) / Data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons attached hereto as **Exhibit C: Intercom Vendor Security Requirements**.

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 5.1 (Current Sub-processors and Notification of Sub-processor Changes) of this DPA.

Intercom agrees that (a) Vendor may engage Sub-processors as listed here:

[Vendor to fill out]

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 organization 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.

EXHIBIT C

Intercom Vendor Security Requirements

These Security Requirements apply to Vendor when it provides services to Intercom. Terms used here but not defined here are defined in the Agreement.

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data	● All data sent to or from Vendor is encrypted in transit using TLS 1.2. ● Intercom Personal Data is encrypted at rest using 256-bit encryption ● All Vendor datastores used to store and/or process Intercom Personal Data are configured and patched using commercially reasonable methods according to industry-recognized system-hardening standards.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	● Vendor implements and maintains a working network firewall to protect data accessible via the Internet and will keep all Intercom Personal Data protected by the firewall at all times. ● Vendor keeps its systems and software up to date with the latest upgrades, updates, bug fixes, new versions and other modifications necessary to ensure security of the Intercom Personal Data. ● Vendor uses anti-malware software and keeps the anti-malware software up to date. ● Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events (e.g., timestamp, originating IP address, transaction completed) are retained for the duration of the Agreement, complying with applicable policies and regulations. Audit logs will be reviewed regularly and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs will be restricted to authorized personnel ● Vendor requires annual security and privacy training for all employees with access to Intercom Personal Data.
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 confidentiality, integrity, availability and resilience of processing systems and services" above.
Processes for regularly testing, assessing, and evaluating the	● Vendor shall maintain compliance with at least one of the following: (i) SOC 2; or (ii) ISO 27001 and provide audit reports or evidence of these certifications to Intercom upon request.

effectiveness of technical and organizational measures in order to ensure the security of the processing	● Vendor shall, at no cost to Intercom, allow for and contribute to audits and make available to Intercom all information necessary, including inspections, conducted by Intercom or another auditor mandated by Intercom for the purpose of demonstrating compliance by Vendor with its obligations under this Agreement. ● Such Assessments will be for the purpose of assessing Vendor's security infrastructure and processes and Vendor's compliance with the terms of the Agreement. Vendor should be prepared to evidence compliance with all areas of the Agreement. Failure to evidence compliance, or, in the event that such Assessment discloses any deficiencies in Vendor's security infrastructure or processes, the parties will use good faith efforts to develop a mutually agreed upon remediation. Thereafter, Vendor will have 30 days (or such other period of time agreed in writing by the parties) to comply with the terms of the remediation plan. ● Upon Intercom’s request, Vendor will provide Intercom copies of, or, access to, its written security policies. Additionally, Vendor will ensure that its subcontractors are in compliance with such policies.
Measures for user identification and authorisation	● Single Sign-On (SSO) ● Logical Access Controls. Vendor assigns a unique ID to each employee and leverages an identity provider to manage access to systems processing Personal Data. ● All access to systems processing Personal Data is protected by Multi Factor Authentication (MFA). ● Vendor restricts access to Personal Data to only those people with a “need-to-know” following least privileges principles. ● Vendor regularly reviews at least every 180 days the list of people and systems with access to Personal Data and removes accounts upon termination of employment or a change in job status that results in employees no longer requiring access to Personal Data. ● Vendor mandates and ensures the use of system-enforced “strong passwords” in accordance with the best practices (described below) on all systems hosting, storing, processing, or that have or control access to Personal Data and will require that all passwords and access credentials are kept confidential and not shared among personnel. ● Passwords must meet the following criteria: a. contain at least 10 characters; b. must contain lowercase and uppercase letters, numbers, and a special character; c. cannot be part of a vendor provided list of common passwords ● Vendor monitors their production systems and implements and maintains security controls and procedures designed to prevent, detect, and respond to identified threats and risks.

	● Strict privacy controls exist in the application code that are designed to ensure data privacy and to prevent one customer from accessing another customer’s data (i.e., logical separation).
Measures for the protection of data during transmission	● See “Measures of pseudonymisation and encryption of personal data” above.
Measures for the protection of data during storage	● Intrusion Prevention. Vendor implements and maintains a working network firewall to protect data accessible via the Internet and will keep all Personal Data protected by the firewall at all times. ● Vendor keeps its systems and software up to date with the latest upgrades, updates, bug fixes, new versions, and other modifications necessary to ensure security of the Personal Data. ● Security Awareness Training. Vendor requires annual security and privacy training for all employees with access to Personal Data. ● Vendor uses anti-malware software and keeps the anti-malware software up to date. Customer instances are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged. ● Endpoint security software ● System inputs recorded via log files ● Access Control Lists (ACL) ● Multi-factor Authentication (MFA)
Measures for ensuring physical security of locations at which personal data are processed	● Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) will be implemented to safeguard sensitive data and information systems. ● Ingress and egress to secure areas will be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel, equipment and resources are allowed access. ● Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises will be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise and loss. ● Vendor will notify Intercom prior to relocation or transfer of hardware, software or data to any off-site premises, other than what is needed for Vendor’s day-to-day activities. ● Policies and procedures governing asset management must be established for secure repurposing of equipment and resources prior to tenant assignment or jurisdictional transport. ●
Measures for ensuring events logging	● See “Measures for the protection of data during storage” above.
Measures for ensuring system configuration,	● Change and Configuration Management. Vendor uses continuous automation for application and operating systems deployment for

including default configuration	new releases. Integration testing and unit testing are done upon every build with safeguards in place for availability and reliability. ● Access Control Policy and Procedures ● Change Management Procedures
Measures for internal IT and IT security governance and management	● Information security management procedures in accordance with the ISO 27001:2013 standard. ● Information-related business operations continue to be carried out in accordance with the ISO27001:2013 standard. ● Information security policy ● Security Breach Response Plan ● Other written security policies include: (a) Business Continuity Policy; (b) Secure Software Development Policy; (c) Electronic Device Policy; (d) Data Classification Policy; (e) Network Security Policy; (f) IT Security Policy; (g) Physical Security Policy; (h) Access Control Policy.
Measures for certification/assurance of processes and products	● See "Measures for internal IT and IT security governance and management".
Measures for ensuring data minimisation	● Data collection is limited to the purposes of processing (or the data that the Customer chooses to provide). ● Security measures are in place to provide only the minimum amount of access (least privilege) necessary to perform required functions. ● Upon termination or expiry of this Agreement, Vendor will delete or return to Intercom all Personal 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 Vendor is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data Vendor will securely isolate and protect from any further processing, except to the extent required by applicable law. ●
Measures for ensuring data quality	● Vendor has a process that allows data subjects to exercise their privacy rights (including a right to amend and update their Personal Data). ● See "Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services" above.
Measures for ensuring limited data retention	● See "Measures for ensuring data minimization" above.
Measures for ensuring accountability	● Vendor has implemented data protection policies ● Vendor follows a compliance by design approach ● Vendor maintains documentation of your processing activities ● Vendor adheres to relevant codes of conduct and signing up to certification schemes (see "Measures for certification/assurance of processes and products" above).

Measures for allowing data portability and ensuring erasure	● See "Measures for ensuring data minimisation". ● Return or Deletion. Vendor will permanently and securely delete all live (online or network accessible) instances of Intercom Personal Data within 30 days upon Intercom request or Agreement termination. ● Archival Copies. When required by law to retain archival copies of Intercom Personal Data for tax or similar regulatory purposes, this archived Intercom Personal Data is stored as a "cold" or offline (i.e., not available for immediate or interactive use) backup stored in a physically secure facility.
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 new third-party service providers or vendors who will have access to Personal Data, Vendor conducts a risk assessment of vendors' data security practices. ● Vendor will restrict the onward sub-processor's access to Personal Data only to what is strictly necessary to provide the Services, and Vendor will prohibit the sub-processor from processing the Personal Data for any other purpose. ● Vendor 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 Personal Data to the standard required by Applicable Data Protection Legislation. ● Vendor will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors. ● the data is encrypted in accordance with this document, and ● the third-party service provider will not have access to the decryption key or unencrypted "plain text" versions of the data. Intercom reserves the right to require an Intercom security review of the third-party service provider before giving approval. ● If Vendor uses any third-party service provider that store or otherwise may access unencrypted Intercom Personal Data, Vendor must perform a security review of the third-party service provider and their security controls and will provide Intercom periodic reporting about the third-party service provider security controls in the format requested by Intercom (e.g. annual SSAE 16 auditing report, or other comparable recognized industry-standard report approved by Intercom).
Misc.	Disaster Recovery. ● Vendor defines and documents a method to replicate Intercom Personal Data over secure links to a disaster recovery site in case of a catastrophic loss. ● Vendor establishes, documents and adopts a consistent unified framework for business continuity planning and plan development to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security

requirements. Business continuity plans will be subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness.

- Physical protection against damage from natural causes and disasters as well as deliberate attacks including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear mishap, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster will be anticipated, designed and countermeasures applied.
- Vendor implements security mechanisms and redundancies to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.).
- Telecommunications equipment, cabling and relays transferring data or supporting services shall be protected from interception or damage and designed with redundancies, alternative power source and alternative routing.
- Application Scans. Vendor performs periodic (but no less than once per month) application vulnerability scans.
- Third party penetration tests. Vendor employs an independent third-party vendor to conduct periodic (but no less than once per year) penetration tests on their web properties.
- Bug bounty program. Vendor agrees that Intercom may make deliverables or results of the Services subject to Intercom's Bug Bounty Program. Intercom will notify Vendor of any material security-related vulnerabilities in the Services or deliverables identified through its Bug Bounty Program. Vendor understands that research and disclosures are governed by Intercom's VDP, which requires good faith and responsible behavior by participants. Vendor bears the cost of any bounty awarded through the Bug Bounty Program for any qualifying finding attributed to their web property based on the reward range listed in https://www.bugcrowd.com/intercom.
- Fixing issues. Vendor will fix all critical and high severity vulnerabilities that could affect the security of Intercom Data, within 7 days of becoming aware of the vulnerability. If Vendor cannot fix the vulnerability within 7 days, Vendor will promptly inform Intercom, including all details of the risk to Intercom arising from Vendor's inability to fix the vulnerability
- Change and Configuration Management. Vendor shall maintain and follow a Secure Development Lifecycle ("SDL") for the development of its products and services. Vendor's SDL will be supported by at least one full time security engineer. Vendor will provide Intercom a copy of its SDL policy and process documents upon request.

EXHIBIT D
Consultant Handbook

Introduction

This Consultant Handbook is comprised of Intercom's Information Security Policy for Consultants and is intended as a reference document for consultants retained by Intercom. The acceptable use polices and behavioral standards provided in this Consultant Handbook are intended to apply to Intercom's consultants whenever they are performing services for or on behalf of Intercom.

Intercom's Information Security Policy (for Consultants)

Intercom's main objectives for information security is to protect the confidentiality, integrity and availability of our own data and our customers' data and maintain customer trust.

As a consultant, you can help Intercom maintain these objectives by adhering to the following policies:

- Consultants and contractors should understand that they have permission to access Intercom's communication systems for work purposes only.

- Consultants and contractors must not share the subject or content of sensitive or confidential data publicly, or via systems or communication channels not managed by Intercom. For example, the use of external e-mail systems not hosted by Intercom to share data is not allowed.

- Consultants and contractors should use a secure password on all systems. These credentials should be unique and should not be used on other external systems or services. Account sharing is prohibited with exceptions for certain vendor applications that are stored in the 1Password vault. Such applications should be approved by Team Security prior to access.

- Consultants and contractors should not use removable media (i.e. USB sticks, portable hard drives, etc.) to handle Intercom data. If you have a question regarding use of a transfer mechanism, please speak to the Security Team via #ask-security on Slack.

- Intercom may provide resources to its consultants and contractors to enable them to perform their job duties. All equipment and supplies, ranging from furniture to various communications systems and technical resources, are provided at Intercom's expense, are Intercom property and must be used only to conduct Intercom business. Consultant-provided equipment must be treated at the same level of Intercom-provided equipment and all applicable policies cover them.

- If you become aware of any risks to Intercom's information security, such as if a device containing Intercom data is lost or stolen (e.g. mobile phones, laptops etc.), please inform the Infosec group via the #ask-security Slack channel, by emailing security@intercom.io or by reaching out directly to a member of the Infosec group or your hiring manager so that we can take appropriate action.

- Thibault Candebat (thibault@intercom.com) is the HIPAA Security Officer and is responsible for implementing HIPAA policies and procedures. You can contact him through email, Slack or reach out to #ask-security for any questions or concerns related to HIPAA.

By taking these measures, we can all help maintain Intercom's information security and data protection commitments and protect our reputation as well as our customers' data.