



Exhibit D-1

INTERCOM MASTER SAAS SUBSCRIPTION AGREEMENT

Customer Name	State Board of Administration of Florida
----------------------	--

AGREEMENT

This Master SaaS Subscription Agreement (“**Agreement**”) is entered into by and between the Intercom entity set forth below (“**Intercom**”) and the customer specified above (“**Customer**”) and is effective as of the date of last signature below (“**Effective Date**”). The Agreement consists of the terms and conditions set forth below, any attachments or exhibits identified below and any Order Forms (as defined below) that reference this Agreement.

This Agreement permits Customer to purchase subscriptions to Services (as defined below) and related Professional Services (as defined below) from Intercom pursuant to mutually executed Intercom order forms referencing this Agreement (“**Order Form(s)**”) and sets forth the basic terms and conditions under which those Services and Professional Services will be delivered. This Agreement will govern Customer’s initial purchase on the Effective Date as well as any future purchases made by Customer that reference this Agreement.

OVERVIEW

Intercom’s Services are a suite of messaging software-as-a-service solutions offered through a single platform. The Services are designed to enable Customer to manage communications with People through the entire lifecycle of their relationship with Customer and to provide a Dashboard for accessing and managing Customer Data regarding those People. Customer may import and export Customer Data between the Services and certain Third-Party Platforms through supported integrations. The Services also include Intercom Code deployed on Customer Properties to enable live chat and messaging functionality.

Accepted and agreed to as of the Effective Date by the authorized representative of each party:

State Board of Administration of Florida
1801 Hermitage Blvd
Tallahassee, Florida 32308
United States

INTERCOM R&D UNLIMITED COMPANY
2nd Floor, Stephen Court, 18-21 St. Stephen’s Green
Dublin 2, Republic of Ireland

Signature

Signature

Print Name

Print Name

Title

Title

Date

Date

Email:

Email:

Primary Contact:

Primary Contact:

1. DEFINITIONS

“**Affiliate**” means any entity under the control of Customer where “**control**” means ownership of or the right to control greater than 50% of the voting securities of such entity.

“**AUP**” means Intercom’s Acceptable Use Policy, available at <https://www.intercom.com/terms-and-policies#aup> or a successor URL.

“**Contractor**” means an independent contractor or consultant who is not a competitor of Intercom.

“**Customer Data**” means any data of any type that is submitted to or accessed by the Services by or on behalf of Customer, including without limitation: (a) data submitted, uploaded or imported to the Services by Customer (including from Third Party Platforms) and (b) data provided by or about Customer or People (including chat and message logs) that are collected from the Customer or Customer Properties using the Services, including the information derived therefrom to the extent Customer is identified (this does not include aggregated, anonymized data).

“**Customer Properties**” means Customer’s websites, apps, or other offerings owned and operated by (or for the benefit of) Customer through which Customer uses the Services to communicate with People.

“**Dashboard**” means Intercom’s user interface for accessing and administering the Services that Customer may access via the web or the Intercom Client Software.

“**Documentation**” means the technical user documentation provided with the Services.

“**Feedback**” means comments, questions, suggestions or other feedback relating to any Intercom product or service.

“**Intercom Client Software**” means any Intercom mobile application or desktop client software provided with the applicable Service.

“**Intercom Code**” means certain JavaScript code, software development kits (SDKs) or other code provided by Intercom for deployment on Customer Properties.

“**Laws**” means all applicable local, state, federal and international laws, regulations and conventions, including, without limitation, those related to data privacy and data transfer, international communications, and the exportation of technical or personal data.

“**Messenger App**” means a type of integration with a Third-Party Platform which a Customer selects and accesses through the Intercom “App Store” or other element of the Services.

“**People**” (in the singular, “**Person**”) means Customer’s end user customers, potential customers, and other users of and visitors to the Customer Properties.

“**Permitted User**” means an employee or Contractor of Customer or its Affiliate who is authorized to access the Service.

“**Sensitive Personal Information**” means any of the following: (i) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards (“**PCI DSS**”); (ii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act (“**HIPAA**”) not authorized or covered by a duly executed Business Associate Agreement with Intercom; or (iii) any other personal data of an EU citizen deemed to be in a “special category” (as identified in EU General Data Protection Regulation or any successor directive or regulation).

“**Services**” means Intercom’s proprietary software-as-a-service solution(s), including the Dashboard, Intercom application programming interfaces (APIs), Intercom Code and Intercom Client Software, as described in the applicable Order Form.

“**Support**” has the meaning set forth in Intercom’s Service Levels and Customer Support Policy.

“**Taxes**” means any sales, use, GST, value-added, withholding, or similar taxes or levies, whether domestic or foreign, other than taxes based on the income of Intercom.

“**Third-Party Platform**” means any software, software-as-a-service, data sources or other products or services not provided by Intercom that are integrated with or otherwise accessible through the Services.

2. INTERCOM SERVICES

2.1. Provision of Services. Each Service is provided on a subscription basis for a set term designated on the Order Form (each, a “**Subscription Term**”). Intercom may also offer Professional Services (as defined in Section 12) related to certain Services. Customer will purchase and Intercom will provide the specific Services and related Professional Services (if any) as specified in the applicable Order Form.

2.2. Access to Services. Customer may access and use the Services solely for its own benefit and in accordance with the terms and conditions of this Agreement, the Documentation and any scope of use restrictions designated in the applicable Order Form (including without limitation the number of People tracked). Use of and access to the Services is permitted only by Permitted Users. If Customer is given API keys or passwords to access the Services on Intercom’s systems, Customer will require that all Permitted Users keep API keys, user ID and password information strictly confidential and not share such information with any unauthorized person. User IDs are granted to individual, named persons and may not be shared. If Customer is accessing the Services using credentials provided by a third party (e.g., Google), then Customer will comply with all applicable terms and conditions of such third party regarding provisioning and use of such credentials. Customer will be responsible for any and all actions taken using Customer’s accounts and passwords. If any Permitted User who has access to a user ID is no longer an employee (or Contractor, as set forth below) of Customer, then Customer will immediately delete such user ID and otherwise terminate such Permitted User’s access to the Service. The right to use the Services includes the right to deploy Intercom Code on Customer Properties in order to enable messaging, chat and similar functionality and to collect Customer Data for use with the Services as further described below.

2.3. Intercom Client Software. To the extent Intercom provides Intercom Client Software for use with the Services, subject to all of the terms and conditions of this Agreement, Intercom grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to use the object code form of the Intercom Client Software internally, but only in connection with Customer’s use of the Service and otherwise in accordance with the Documentation and this Agreement.

2.4. Deployment of Intercom Code. Subject to all of the terms and conditions of this Agreement, Intercom grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to copy the Intercom Code in the form provided by Intercom on Customer Properties solely to support Customer’s use of the Service and otherwise in accordance with the Documentation and this Agreement. Customer must implement Intercom Code on the Customer Properties in order to enable features of the Services. Customer will implement all Intercom Code in strict accordance with the Documentation and

other instructions provided by Intercom. Customer acknowledges that any changes made to the Customer Properties after initial implementation of Intercom Code may cause the Services to cease working or function improperly and that Intercom will have no responsibility for the impact of any such Customer changes.

2.5. Contractors and Affiliates. Customer may permit its Contractors and its Affiliates' employees and Contractors to serve as Permitted Users, provided Customer remains responsible for compliance by such individuals with all of the terms and conditions of this Agreement, and any use of the Services by such individuals is for the sole benefit of Customer.

2.6. General Restrictions. Customer will not (and will not permit any third party to): (a) rent, lease, provide access to or sublicense the Services to a third party; (b) use the Services to provide, or incorporate the Services into, any product or service provided to a third party; (c) reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code or non-public APIs to the Services, except to the extent expressly permitted by applicable law (and then only upon advance notice to Intercom); (d) copy or modify the Services or any Documentation, or create any derivative work from any of the foregoing; (e)

2.7. Intercom APIs. If Intercom makes access to any APIs available as part of the Services, Intercom reserves the right to place limits on access to such APIs (e.g., limits on numbers of calls or requests). Further, Intercom may monitor Customer's usage of such APIs and limit the number of calls or requests Customer may make if Intercom believes that Customer's usage is in breach of this Agreement or may negatively affect the Services (or otherwise impose liability on Intercom).

2.8. Trial Subscriptions. If Customer receives free access or a trial or evaluation subscription to the Service (a "Trial Subscription"), then Customer may use the Services in accordance with the terms and conditions of this Agreement for a period of fourteen (14) days or such other period granted by Intercom (the "Trial Period"). Trial Subscriptions are permitted solely for Customer's use to determine whether to purchase a paid subscription to the Services. Trial Subscriptions may not include all functionality and features accessible as part of a paid Subscription Term. If Customer does not enter into a paid Subscription Term, this Agreement and Customer's right to access and use the Services will terminate at the end of the Trial Period. Intercom has the right to terminate a Trial Subscription at any time for any reason. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, INTERCOM WILL HAVE NO WARRANTY, INDEMNITY, SUPPORT, OR OTHER OBLIGATIONS WITH RESPECT TO TRIAL SUBSCRIPTIONS.

3. CUSTOMER DATA

3.1. Rights in Customer Data. As between the parties, Customer Data will remain the exclusive property of the Customer, and Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data as provided to Intercom. Subject to the terms of this Agreement, Customer hereby grants to Intercom a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data solely to the extent necessary to provide the Services to Customer. Intercom shall provide to Customer, upon its request, access to and the ability to download Customer Data. Intercom will not sell, assign, lease, or

otherwise transfer any Customer Data to third parties, or commercially exploit Customer Data, except as authorized in writing by the Customer. For the avoidance of doubt, Customer authorizes Intercom to provide Customer Data to People in the regular course of providing Services. Intercom will not possess or assert any lien or other right against or to any Customer Data in any circumstances.

3.2. Storage of Customer Data. Intercom does not provide an archiving service but does agree to protect the Customer Data as outlined in Section 14 of this Agreement, the DPA (Exhibit C), and the Terms Addendum (Exhibit D). Intercom agrees that it will not intentionally delete any Customer Data from any Service prior to termination of Customer's applicable Subscription Term except at Customer's direction. Notwithstanding anything to the contrary in this Agreement, Intercom further agrees that, upon Customer's direction and request, Intercom will delete Customer Data, including all copies and back-ups in any format in the time frame provided for in this Agreement.

3.3. Customer Obligations.

a) **In General.** Customer is solely responsible for the accuracy, content and legality of all Customer Data. Customer represents and warrants to Intercom that Customer has all necessary rights, consents and permissions to collect, share and use all Customer Data as contemplated in this Agreement (including granting Intercom the rights in Section 3.1 (Rights in Customer Data)) and that no Customer Data will violate or infringe (i) any third party intellectual property, publicity, privacy or other rights, (ii) any Laws, or (iii) any terms of service, privacy policies or other agreements governing the Customer Properties or Customer's accounts with any Third-Party Platforms. Customer further represents and warrants that all Customer Data complies with the AUP. As between the parties, Customer will be fully responsible for any Customer Data submitted to the Services by any Person as if it was submitted by Customer.

b) **No Sensitive Personal Information.** Customer specifically agrees not to use the Services to collect, store, process or transmit any Sensitive Personal Information unless expressly authorized by Intercom and with respect to PHI, unless Customer has also entered into a Business Associate Agreement with Intercom. Customer acknowledges that Intercom is not PCI DSS compliant. Intercom will have no liability under this Agreement for Sensitive Personal Information, notwithstanding anything to the contrary herein.

c) **Compliance with Laws.** Customer agrees to comply with all applicable Laws in its use of the Services. Without limiting the generality of the foregoing, Customer will not engage in any unsolicited advertising, marketing, or other activities using the Services, including without limitation any activities that violate the Telephone Consumer Protection Act of 1991, CAN-SPAM Act of 2003 or any other anti-spam laws and regulations.

d) **Disclosures on Customer Properties.** Customer acknowledges that the Intercom Code causes a unique cookie ID to be associated with each Person who accesses the Customer Properties, which cookie ID enables Intercom to provide the Services. Customer will include on each Customer Property a link to its privacy policy that discloses Customer's use of third party tracking technology to collect data about People as described in this Agreement. Customer's privacy policy must disclose how, and for what purposes, the data collected through third party code will be used or shared with third parties. Customer must also provide People with clear and comprehensive information about the storing and accessing of cookies. For clarity, as between Customer and Intercom, Customer will be solely responsible for obtaining the necessary clearances, consents and approvals from People under all applicable Laws.

e) **Intentionally Omitted**

3.4. Indemnification by Customer. Customer will indemnify, defend and hold harmless Intercom from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with any claim arising from or relating to any Customer Data (unless such claim is related to Intercom's breach or alleged breach of this Agreement) or breach or alleged breach by Customer of Section 3.3 (Customer Obligations). This indemnification obligation is subject to Customer receiving (i) prompt written notice of such claim (but in any event notice in sufficient time for Customer to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense, or settlement of such claim; and (iii) all necessary cooperation of Intercom at Customer's expense. Notwithstanding the foregoing sentence, (a) Intercom may participate in the defense of any claim by counsel of its own choosing, at its cost and expense and (b) Customer will not settle any claim without Intercom's prior written consent, unless the settlement fully and unconditionally releases Intercom and does not require Intercom to pay any amount, take any action, or admit any liability. Notwithstanding the above, this indemnity is the sole and exclusive remedy of Intercom for any third party claim relating to the Customer Data. Notwithstanding the above, this section is applicable only to the extent permitted by Florida law.

3.5. Aggregated Anonymous Data. Notwithstanding anything to the contrary herein, Customer agrees that Intercom may obtain and aggregate technical and other data about Customer's use of the Services that is non-personally identifiable with respect to Customer ("Aggregated Anonymous Data"), and Intercom may use the Aggregated Anonymous Data to analyze, improve, support and operate the Services and otherwise for any business purpose during and after the term of this Agreement, including without limitation to generate industry benchmark or best practice guidance, recommendations or similar reports for distribution to and consumption by Customer and other Intercom customers. For clarity, this Section 3.5 does not give Intercom the right to identify Customer as the source of any Aggregated Anonymous Data.

3.6. EU-U.S. Privacy Shield. This Section 3.6 applies only if Customer has entered into this Agreement with Intercom, Inc. as set forth above. Intercom, Inc. participates in the EU-U.S. Privacy Shield framework. For more information, please see Intercom's EU-U.S. Privacy Shield Statement, available at <https://www.intercom.com/privacy/eu-us-privacy-shield-policy> or a successor URL.

3.7. Data Protection. Under this Agreement, Intercom may obtain certain information relating to identified or identifiable individuals ("Personal Data"). The Data Protection Addendum ("DPA") attached hereto as Exhibit C, along with other provisions of this Agreement, will govern Intercom's access to Personal Data.

4. SECURITY. Intercom has established appropriate administrative, technical, and physical safeguards to protect the confidentiality of, and to prevent the unauthorized use or access to, Customer Data in accordance with the Security Policy set forth in the DPA ("Security Policy"). Intercom shall develop data security procedures designed to ensure only authorized access to data and databases by Intercom representatives for purposes of performing the Agreement and designed to ensure no unauthorized access to data or databases by individuals or entities other than those authorized by the Agreement or Customer. Intercom shall ensure that access to data and databases by Intercom representatives will be provided on a need to know basis and will adhere to the principle of least privilege. (The principle of least privileged means giving a user account only those privileges which are essential to perform its intended function.) The parties further agree to the terms set forth in the Terms Addendum, which is hereby incorporated into this Agreement as Exhibit D.

5. THIRD-PARTY PLATFORMS AND MESSENGER APPS. The Services support integrations (including Messenger Apps) with certain Third-Party Platforms. To enable the Services to access and receive Customer's information from a Third-Party Platform, Customer may be required to input its credentials for such Third-Party Platform. By enabling use of the Services with any Third-Party Platform, Customer authorizes Intercom to access Customer's accounts with such Third-Party Platform for the purposes described in this Agreement. Customer is solely responsible for complying with any relevant terms and conditions of the Third-Party Platforms or otherwise presented by the providers of Messenger Apps and for maintaining appropriate accounts in good standing with the providers of the Third-Party Platforms. Customer acknowledges and agrees that Intercom has no responsibility or liability for any Third-Party Platform or Messenger App, or any Customer Data exported to, accessed or used by a Third-Party Platform or Messenger App. Intercom does not guarantee that the Services will maintain integrations with any Third-Party Platform and Intercom may disable integrations of the Services with any Third-Party Platform (including Messenger Apps) at any time with or without notice to Customer. For clarity, this Agreement governs Customer's use of and access to the Services, even if accessed through an integration with a Third-Party Platform.

6. OWNERSHIP.

6.1. Intercom Technology. This is a subscription agreement for access to and use of the Services. Customer acknowledges that it is obtaining only a limited right to the Services and that irrespective of any use of the words "purchase", "sale" or like terms in this Agreement no ownership rights are being conveyed to Customer under this Agreement. Customer agrees that Intercom or its suppliers retain all right, title and interest (including all patent, copyright, trademark, trade secret and other intellectual property rights) in and to the Services and all Documentation, professional services deliverables and any and all related and underlying technology and documentation and any derivative works, modifications or improvements of any of the foregoing, including as may incorporate Feedback (collectively, "Intercom Technology"). Except as expressly set forth in this Agreement, no rights in any Intercom Technology are granted to Customer.

6.2. Feedback. Customer, from time to time, may submit Feedback to Intercom. Intercom may freely use or exploit Feedback in connection with any of its products or services.

7. SUBSCRIPTION TERM, FEES & PAYMENT

7.1. Subscription Term and Renewals. Unless otherwise specified on the applicable Order Form, each Subscription Term will automatically renew for additional twelve month periods unless either party gives the other written notice of termination at least thirty (30) days prior to expiration of the then-current Subscription Term.

7.2. Fees and Payment. All fees are as set forth in the applicable Order Form and will be paid by Customer within thirty (30) days of invoice, unless (a) Customer is paying via Credit Card (as defined below) or (b) otherwise specified in the applicable Order Form. Except as expressly set forth in Section 8.2 (Termination for Cause), Section 9 (Limited Warranty) and Section 14 (Indemnification), all fees are non-refundable. Customer is responsible for paying all applicable Taxes, and all Taxes are excluded from any fees set forth in the applicable Order Form. If Customer is required by Law to withhold any Taxes from Customer's payment, the fees payable by Customer will be increased as necessary so that after making any required withholdings, Intercom receives and retains (free from any liability for payment of Taxes) an amount equal to the amount it would have received had no such withholdings been made. Any late payments will be subject to a service charge equal to 1.5% per month

of the amount due or the maximum amount allowed by law, whichever is less.

7.3. Payment Via Credit Card. If you are purchasing the Services via credit card, debit card or other payment card ("Credit Card"), the following terms apply:

a) **Recurring Billing Authorization.** By providing Credit Card information and agreeing to purchase any Services, Customer hereby authorizes Intercom (or its designee) to automatically charge Customer's Credit Card on the same date of each calendar month (or the closest prior date, if there are fewer days in a particular month) during the Subscription Term for all fees accrued as of that date (if any) in accordance with the applicable Order Form. Customer acknowledges and agrees that the amount billed and charged each month may vary depending on Customer's use of the Services and may include subscription fee adjustments charged in advance for the remainder of Customer's applicable billing period and overage fees for the prior month.

b) **Foreign Transaction Fees.** Customer acknowledges that for certain Credit Cards, the issuer of Customer's Credit Card may charge a foreign transaction fee or other charges.

c) **Invalid Payment.** If a payment is not successfully settled due to expiration of a Credit Card, insufficient funds, or otherwise, Customer remains responsible for any amounts not remitted to Intercom and Intercom may, in its sole discretion, (i) invoice Customer directly for the deficient amount, (ii) continue billing the Credit Card once it has been updated by Customer (if applicable) or (iii) terminate this Agreement.

d) **Changing Credit Card Information.** At any time, Customer may change its Credit Card information by entering updated Credit Card information via the "Settings" page on the Dashboard.

e) **Termination of Recurring Billing.** Customer may terminate its Subscription Term in accordance with Section 7.1 (Subscription Term and Renewals). Upon any termination or expiration of the Subscription Term, Intercom will charge Customer's Credit Card (or invoice Customer directly) for any outstanding fees for Customer's use of the Services prior to such termination, after which Intercom will not charge Customer's Credit Card for any additional fees for the terminated Subscription Term.

7.4. Suspension of Service. Without limiting Intercom's termination or other rights hereunder, Intercom reserves the right to suspend Customer's access to the applicable Service (and any related Professional Services and Support) in whole or in part, without liability to Customer: (i) if Customer's account is thirty (30) days or more overdue; (ii) if Customer's use of the Services is in violation of the AUP; (iii) for Customer's breach of Sections 2.6 (General Restrictions) or 3.3 (Customer Obligations); or (iv) to prevent harm to other customers or third parties or to preserve the security, availability or integrity of the Services (including if Customer is or becomes listed on any reputable blacklist, blocklist, or similar list of spam abusers). Unless this Agreement has been terminated, Intercom will restore Customer's access to the Services promptly after Intercom verifies to its satisfaction that Customer has resolved the issue requiring suspension and there is no likelihood of ongoing violation.

8. TERM AND TERMINATION

8.1. Term. This Agreement is effective as of the Effective Date and expires on the date of expiration or termination of all Subscription Terms.

8.2. Termination for Cause. Either party may terminate this Agreement (including all related Order Forms) if the other party (a) fails to cure any material breach of this Agreement (including with respect to Customer any of the events set forth in Section 7.4 (Suspension)) within thirty (30) days after written notice; (b) ceases operation without a successor; (c) seeks protection under any bankruptcy, receivership, trust deed, creditors' arrangement, composition, or comparable proceeding, or if any such proceeding is instituted against that party (and not dismissed within sixty (60) days thereafter), or (d) is required to pursuant to applicable law, including Florida law. Notwithstanding the foregoing, Customer may terminate this Agreement without notice and no opportunity to cure following any breach of personal identifying information in possession of Intercom or any of Intercom's agents, contractors, subcontractors, subprocessors or consultants, including affiliates (hereinafter "Intercom Representatives"). If Customer terminates the Agreement pursuant to this section 8.2, Customer shall be entitled to a pro-rata refund of all fees paid by Customer to Intercom.

8.3. Effect of Termination. Upon any expiration or termination of this Agreement, Customer will immediately cease any and all use of and access to all Services (including any and all related Intercom Technology) and delete (or, at Intercom's request, return) any and all copies of the Documentation, any Intercom passwords or access codes and any other Intercom Confidential Information in its possession. Provided this Agreement was not terminated for Customer's breach, Customer may retain and use internal copies of all reports exported from any Service prior to termination. Customer acknowledges that following termination it will have no further access to any Customer Data input into any Service, and that Intercom may delete any such data as may have been stored by Intercom at any time. Except where an exclusive remedy is specified, the exercise of either party of any remedy under this Agreement, including termination, will be without prejudice to any other remedies it may have under this Agreement, by law or otherwise. This section is applicable to the extent permitted by Florida law.

8.4. Survival. The following Sections will survive any expiration or termination of this Agreement: 2.6 (General Restrictions), 2.8 (Trial Subscriptions), 3.2 (Storage of Customer Data), 3.4 (Indemnification by Customer), 3.5 (Aggregated Anonymous Data), 6 (Ownership), 7.2 (Fees and Payment), 7.3 (Payment Via Credit Card), 8 (Term and Termination), 9.2 (Warranty Disclaimer), 13 (Limitation of Remedies and Damages), 14 (Indemnification), 15 (Confidential Information) and 18 (General Terms). The provision of Section 1.6 of the Terms Addendum (Right to Audit) will survive any termination or expiration of the Agreement and will continue in effect as provided therein. In addition, Section 2 of Exhibit D, Terms Addendum, will survive any termination or expiration of the Agreement and will continue in effect until all Customer Data has been returned to the Customer (if so directed by the Customer) and all Customer Data retained by Intercom has been destroyed.

9. LIMITED WARRANTY

9.1. Limited Warranty. Intercom warrants, for Customer's benefit only, that each Service will operate in substantial conformity with the applicable Documentation. Intercom's sole liability (and Customer's sole and exclusive remedy) for any breach of this warranty will be, at no charge to Customer, for Intercom to use commercially reasonable efforts to correct the reported non-conformity, or if Intercom determines such remedy to be impracticable, either party may terminate the applicable Subscription Term and Customer will receive as its sole remedy a refund of any fees Customer has pre-paid for use of such Service for the terminated portion of the applicable Subscription Term. The limited warranty set forth in this Section 9.1 will not apply: (i) unless Customer makes a claim within thirty (30) days of the date on which

Customer first noticed the non-conformity, (ii) if the error was caused by misuse, unauthorized modifications or third-party hardware, software or services, or (iii) to use provided on a no-charge, trial or evaluation basis.

9.2. Warranty Disclaimer. EXCEPT FOR THE LIMITED WARRANTY IN SECTION 9.1, ALL SERVICES, SUPPORT, AND PROFESSIONAL SERVICES ARE PROVIDED "AS IS". NEITHER INTERCOM NOR ITS SUPPLIERS MAKES ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. INTERCOM DOES NOT WARRANT THAT CUSTOMER'S USE OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, NOR DOES INTERCOM WARRANT THAT IT WILL REVIEW THE CUSTOMER DATA FOR ACCURACY OR THAT IT WILL PRESERVE OR MAINTAIN THE CUSTOMER DATA WITHOUT LOSS OR CORRUPTION. INTERCOM SHALL NOT BE LIABLE FOR THE RESULTS OF ANY COMMUNICATIONS SENT OR ANY COMMUNICATIONS THAT WERE FAILED TO BE SENT USING THE SERVICES. INTERCOM SHALL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES, THIRD-PARTY PLATFORMS OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF INTERCOM. CUSTOMER MAY HAVE OTHER STATUTORY RIGHTS, BUT THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE SHORTEST PERIOD PERMITTED BY LAW. THIS SECTION IS APPLICABLE TO THE EXTENT NOT LIMITED OR PROHIBITED BY FLORIDA LAW.

10. AVAILABILITY AND SERVICE LEVELS. The Services are available subject to Exhibit B (Service Levels and Customer Support).

11. SUPPORT. During the Subscription Term of each Service, Intercom will provide Support in accordance with the terms set forth on Exhibit B (Service Levels and Customer Support).

12. PROFESSIONAL SERVICES. Intercom will provide the professional consulting services ("Professional Services") purchased in the applicable Order Form. The scope of Professional Services will be as set forth in a Statement of Work referencing this Agreement and executed by both parties describing the work to be performed, fees and any applicable milestones, dependencies and other technical specifications or related information ("SOW"). Unless Professional Services are provided on a fixed-fee basis, Customer will pay Intercom at the per-hour rates set forth in the Order Form (or, if not specified, at Intercom's then-standard rates) for any excess services. Any travel expenses incurred by Intercom will need to be approved in writing by Customer in advance of incurring the expenses, and all such travel expenses must be in compliance with Section 112.061, Florida Statutes. Customer may use anything delivered as part of the Professional Services in support of authorized use of the Services and subject to the terms regarding Customer's rights to use the Service set forth in Section 2 (Intercom Services) and the applicable SOW, but Intercom will retain all right, title and interest in and to any such work product, code or deliverables and any derivative, enhancement or modification thereof created by Intercom (or its agents).

13. LIMITATION OF REMEDIES AND DAMAGES

13.1. Consequential Damages Waiver. EXCEPT FOR EXCLUDED CLAIMS, NEITHER PARTY (NOR ITS SUPPLIERS) SHALL HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOSS OF USE, LOST PROFITS, INTERRUPTION OF BUSINESS, OR

ANY INDIRECT, SPECIAL, INCIDENTAL, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. THIS SECTION IS APPLICABLE TO THE EXTENT NOT PROHIBITED OR LIMITED BY FLORIDA LAW.

13.2. Liability Cap. INTERCOM'S AND ITS SUPPLIERS' ENTIRE LIABILITY TO CUSTOMER ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED IN AGGREGATE THE AMOUNT ACTUALLY PAID BY CUSTOMER TO INTERCOM DURING THE PRIOR TWELVE (12) MONTHS UNDER THIS AGREEMENT. THIS SECTION DOES NOT APPLY TO A BREACH OF CUSTOMER DATA. THIS SECTION IS APPLICABLE TO THE EXTENT NOT PROHIBITED OR LIMITED BY FLORIDA LAW.

13.3. Excluded Claims. "Excluded Claims" means any claim arising (a) from Customer's breach of Section 2.6 (General Restrictions); (b) under Section 3.3 (Customer Obligations) or 3.4 (Indemnification by Customer) (if applicable) or 14 (Indemnification by Intercom); or (c) from a party's breach of its obligations in Section 15 (Confidential Information).

13.4. Special Liability Cap.



13.5. Nature of Claims and Failure of Essential Purpose. The parties agree that the waivers and limitations specified in this Section 13 apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy specified in this Agreement is found to have failed of its essential purpose. This section is applicable to the extent not prohibited or limited by Florida law.

14. INDEMNIFICATION. Intercom will defend Customer from and against any claim by a third party alleging that a Service when used as authorized under this Agreement infringes a U.S. patent, U.S. copyright, or U.S. trademark and will indemnify and hold harmless Customer from and against any damages and costs finally awarded against Customer or agreed in settlement by Intercom (including reasonable attorneys' fees) resulting from such claim, provided that Intercom will have received from Customer: (i) prompt written notice of such claim (but in any event notice in sufficient time for Intercom to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense and settlement (if applicable) of such claim; and (iii) all reasonable necessary cooperation of Customer. If Customer's use of a Service is (or in Intercom's opinion is likely to be) enjoined, if required by settlement or if Intercom determines such actions are reasonably necessary to avoid material liability, Intercom may, in its sole discretion: (a) substitute substantially functionally similar products or services; (b) procure for Customer the right to continue using such Service; or if (a) and (b) are not commercially reasonable, (c)

terminate this Agreement and refund to Customer the fees paid by Customer for the portion of the Subscription Term that was paid by Customer but not rendered by Intercom. The foregoing indemnification obligation of Intercom will not apply: (1) if such Service is modified by any party other than Intercom, but solely to the extent the alleged infringement is caused by such modification; (2) if such Service is combined with products or processes not provided by Intercom, but solely to the extent the alleged infringement is caused by such combination; (3) to any unauthorized use of such Service; (4) to any action arising as a result of Customer Data or any third-party deliverables or components contained within such Service; (5) to the extent the alleged infringement is not caused by the particular technology or implementation of the Service but instead by features common to any similar product or service; or (6) if Customer settles or makes any admissions with respect to a claim without Intercom's prior written consent. THIS SECTION 14 SETS FORTH INTERCOM'S AND ITS SUPPLIERS' SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

Intercom agrees to protect, indemnify, defend and hold harmless Customer, its trustees, officers and employees from and against any and all costs, claims, demands, damages, losses, liabilities and expenses (including reasonable counsel fees and expenses, and investigation, collection, settlement and litigation costs) resulting or arising from or in any way related to Intercom's grossly negligent acts or omissions, fraud, or willful misconduct.

15. CONFIDENTIAL INFORMATION. Each party (as "Receiving Party") agrees that all code, inventions, know-how, business, technical and financial information it obtains from the disclosing party ("Disclosing Party") constitute the confidential property of the Disclosing Party ("Confidential Information"), provided that it is identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be confidential or proprietary due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any Intercom Technology, performance information relating to any Service, and the terms and conditions of this Agreement will be deemed Confidential Information of Intercom without any marking or further designation. Except as expressly authorized herein, the Receiving Party will (1) hold in confidence and not disclose any Confidential Information to third parties and (2) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement. The Receiving Party may disclose Confidential Information to its employees, agents, contractors and other representatives having a legitimate need to know (including, for Intercom, the subcontractors referenced in Section 18.8 (Subcontractors)), provided that such representatives are bound to confidentiality obligations no less protective of the Disclosing Party than as set forth in this Agreement and that the Receiving Party remains responsible for compliance by any such representative with the as set forth in this Agreement. The Receiving Party's confidentiality obligations will not apply to information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the Receiving Party who had no access to such information. The Receiving Party may make disclosures to the extent required by law or court order, provided the Receiving Party notifies the Disclosing Party in advance and cooperates in any effort to obtain confidential treatment. The Receiving Party acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a

sufficient remedy, and therefore that upon any such disclosure by the Receiving Party the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

16. MARKETING. Intercom may not identify the Customer for purposes of business development or press releases without express written consent of the Customer.

17. INSURANCE

(i) **General Liability Insurance.** Intercom shall maintain, during the term of this Agreement, no less than the following General Liability Insurance coverage: \$1,000,000 each occurrence, \$2,000,000 aggregate;

(ii) **Workers' Compensation Insurance.** Intercom shall maintain, during the term of this Agreement, statutorily-required Workers' Compensation Insurance or its substantial equivalent on its employees engaged in work related to the performance of this Agreement and Employers Liability limits of no less than \$1,000,000 per employee for bodily injury by accident, 1,000,000 policy limit for bodily injury by disease, and \$1,000,000 per employee for bodily injury by disease on its employees engaged in work directly related to the performance of this Agreement;

(iii) **Umbrella.** Intercom shall maintain, during the term of this Agreement, no less than the following Umbrella Liability Insurance coverage: \$4,000,000 each Occurrence;

(iv) **Technology Errors and Omissions and Cyber Liability.** Intercom shall maintain, during the term of this Agreement, technology errors and omissions liability coverage with minimum limits of \$5,000,000 in the aggregate which shall include coverage for Technology Errors & Omissions. Intercom confirms that this policy covers the following in the event of a breach of data held by Intercom or Intercom's subcontractors: notification, credit monitoring and identity theft protection for affected individuals.

Certificates. If requested in writing by Customer, Intercom shall provide to Customer evidence of the above insurance policies upon the execution of this Agreement and upon any policy renewal thereafter, on a standard ACORD form. Intercom shall provide to Customer not less than thirty (30) days' notice of any cancellation or non-renewal of any of the above insurance policies. The insurance certificates shall reflect the following changes to standard language. Customer shall be named as an additional insured on the policies listed in sections (i) through (iv) above. Customer shall be listed on these policies as follows: State Board of Administration of Florida; 1801 Hermitage Blvd., Ste. 100; Tallahassee, FL 32308.

18. GENERAL TERMS

18.1. Assignment. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement without the advance written consent of the other party, except that either party may assign this Agreement in connection with a merger, reorganization, acquisition or other transfer of all or substantially all of such party's assets or voting securities. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section 18.1 will be null and void.

18.2. Severability. If any provision of this Agreement will be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in effect.

18.3. Dispute Resolution.

a) **Direct Dispute Resolution.** In the event of any dispute, claim, question, or disagreement arising from or relating to this Agreement, whether arising in contract, tort or otherwise, ("Dispute"), the

parties shall use their best efforts to resolve the Dispute. Any notices required to be sent to Intercom regarding a dispute shall be sent to Intercom at legal@intercom.io and sent via mail to:

Attn: Legal Department
Intercom
55 Second Street, Suite 400
San Francisco, CA 94105

Notice to the Customer shall be as set forth in 18.4 below with a copy to:

State Board of Administration of Florida
1801 Hermitage Blvd., Ste. 100
Tallahassee, FL 32308
Attn: General Counsel

18.4. Notice. Any notice or communication required or permitted under this Agreement will be in writing to the parties at the addresses set forth on the Order Form or at such other address as may be given in writing by either party to the other in accordance with this Section and will be deemed to have been received by the addressee (i) if given by hand, immediately upon receipt; (ii) if given by overnight courier service, the first business day following dispatch or (iii) if given by registered or certified mail, postage prepaid and return receipt requested, the second business day after such notice is deposited in the mail.

18.5. Amendments; Waivers. No supplement, modification, or amendment of this Agreement will be binding, unless executed in writing by a duly authorized representative of each party to this Agreement. No waiver will be implied from conduct or failure to enforce or exercise rights under this Agreement, nor will any waiver be effective unless in a writing signed by a duly authorized representative on behalf of the party claimed to have waived. No provision of any purchase order or other business form employed by Customer will supersede the terms and conditions of this Agreement, and any such document relating to this Agreement will be for administrative purposes only and will have no legal effect.

18.6. Entire Agreement. This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement. Customer acknowledges that the Services are on-line, subscription-based products, and that in order to provide improved customer experience Intercom may make changes to the Services, and Intercom will update the applicable Documentation accordingly. The support, security and service level availability terms described in Section 11 (Support), Exhibit A (Intercom Security Policy) and Exhibit B (Service Levels and Customer Support) may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices (but the modifications will not materially decrease Intercom's obligations as compared to those reflected in such terms as of the Effective Date).

18.7. Force Majeure. Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events that occur after the signing of this Agreement and that are beyond the reasonable control of such party, such as a strike, blockade, war, act of terrorism, riot, natural disaster, failure or diminishment of power or telecommunications or data networks or services, or refusal of a license by a government agency. This section is applicable only to the extent all reasonable and diligent

precautions by Intercom could not have prevented delay or failure resulting from any such event.

18.8. Subcontractors. Intercom may use the services of subcontractors and permit them to exercise the rights granted to Intercom in order to provide the Services under this Agreement, provided that Intercom remains responsible for (i) compliance of any such subcontractor with the terms of this Agreement and (ii) for the overall performance of the Services as required under this Agreement.

18.9. Subpoenas. Nothing in this Agreement prevents Intercom from disclosing Customer Data to the extent required by law, subpoenas, or court orders, but Intercom will use commercially reasonable efforts to notify Customer in advance of any disclosure where permitted to do so.

18.10. Independent Contractors. The parties to this Agreement are independent contractors. There is no relationship of partnership, joint venture, employment, franchise or agency created hereby between the parties. Neither party will have the power to bind the other or incur obligations on the other party's behalf without the other party's prior written consent.

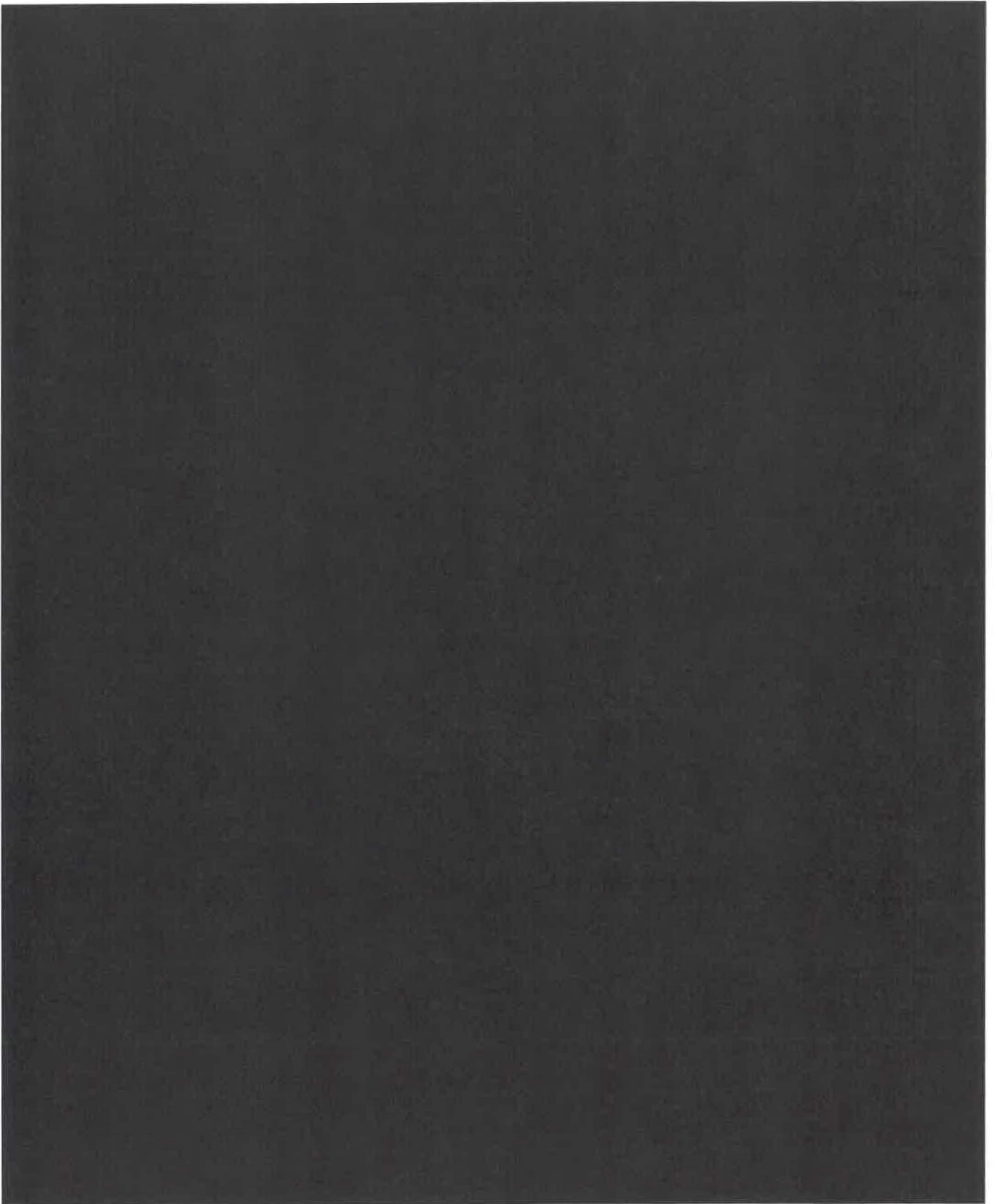
18.11. Export Control. In its use of the Services, Customer agrees to comply with all export and import laws and regulations of the United States and other applicable jurisdictions. Without limiting the foregoing, (i) Customer represents and warrants that it is not listed on any U.S. government list of prohibited or restricted parties or located in (or a national of) a country that is subject to a U.S. government embargo or that has been designated by the U.S. government as a "terrorist supporting" country, (ii) Customer will not (and will not permit any of its users to) access or use the Services in violation of any U.S. export embargo, prohibition or restriction, and (iii) Customer will not submit to the Services any information that is controlled under the U.S. International Traffic in Arms Regulations.

18.12. Government End-Users. Elements of the Services are commercial computer software. If the user or licensee of the Services is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Services, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. All Services were developed fully at private expense. All other use is prohibited.

18.13. Counterparts. This Agreement may be executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.



Exhibit A



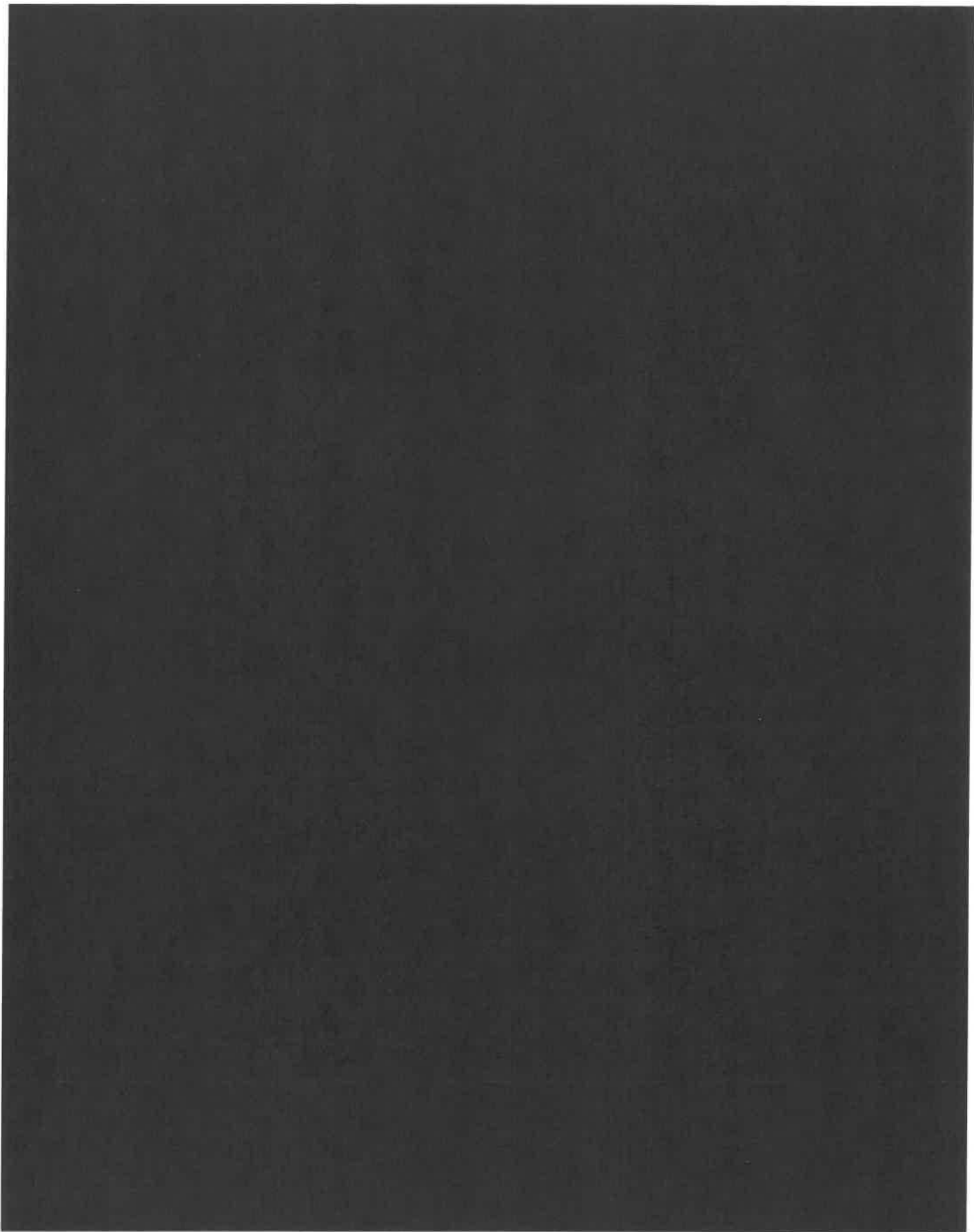
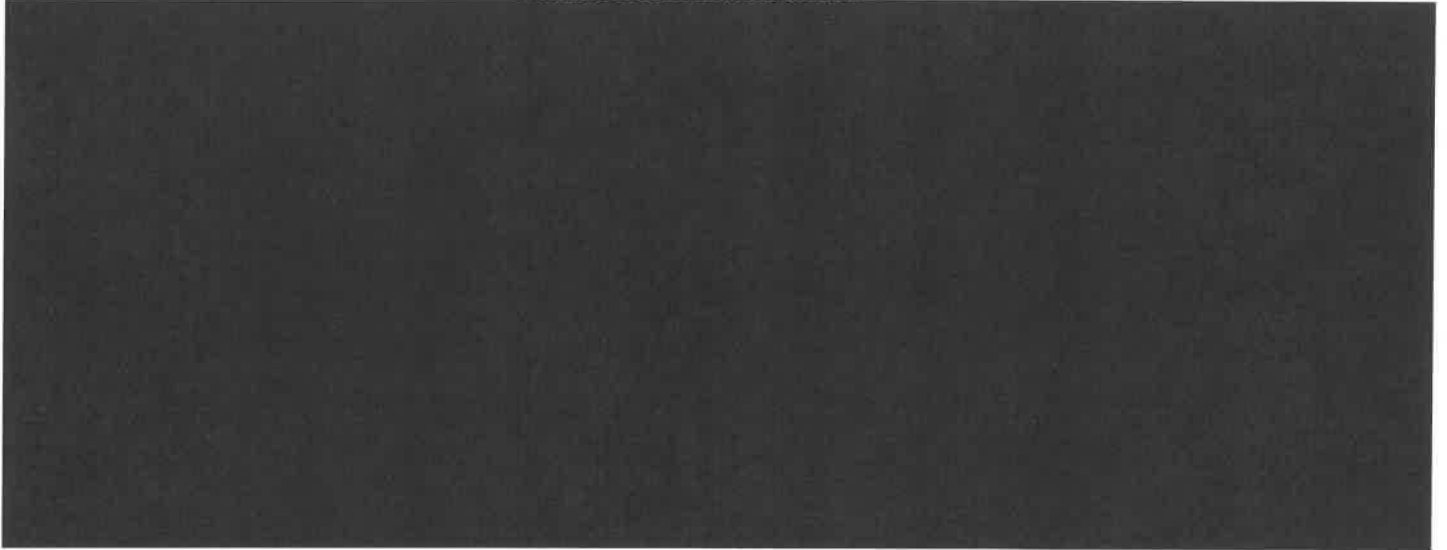


Exhibit B

SERVICE LEVELS AND CUSTOMER SUPPORT

Intercom Service Level Agreement



Intercom Support Policy

Intercom offers support services for the Service ("Support") in accordance with the following terms:

- A. **Support Hours.** Support is provided 24 hours per day, 7 days per week.
- B. **Incident Submission and Customer Cooperation.** Customer may report errors or abnormal behavior of the Service ("Incidents") by contacting Intercom in the Service via the Intercom Messenger or via email at team@intercom.com. Customer will provide information and cooperation to Intercom as reasonably required for Intercom to provide Support. This includes, without limitation, providing the following information to Intercom regarding the Incident:
- Aspects of the Service that are unavailable or not functioning correctly
 - Incident's impact on users
 - Start time of Incident
 - List of steps to reproduce Incident
 - Relevant log files or data
 - Wording of any error message
- C. **Incident Response.** Intercom's Support personnel will assign a priority level ("Priority Level") to each Incident and seek to provide responses in accordance with the table below.

<u>Priority Level</u>	<u>Description</u>	<u>Target Response Times</u>
Priority 1	Operation of the Service is critically affected (not responding to requests or serving content) for a large number of users; no workaround available.	2 Hours
Priority 2	Service is responding and functional but performance is degraded, and/or Incident has potentially severe impact on operation of the Service for multiple users.	1 Day
Priority 3	Non-critical issue; no significant impact on performance of the Service but user experience may be affected.	3 Days

- D. **Exclusions.** Intercom will have no obligation to provide Support to the extent an Incident arises from: (a) use of the Service by Customer in a manner not authorized in the Agreement or the applicable Documentation; (b) general Internet problems, force majeure events or other factors outside of Intercom's reasonable control; (c) Customer's equipment, software, network connections or other infrastructure; or (d) third party systems, acts or omissions (excluding Intercom Representatives).

Exhibit C

Data Processing Addendum (DPA)

This Data Processing Addendum, including its annexes and the Standard Contractual Clauses, ("DPA") is made by and between Intercom R&D Unlimited Company ("Intercom"), and Customer, pursuant to the Master SaaS Subscription Agreement ("Agreement").

This DPA forms part of the Agreement and sets out the terms that apply when Personal Data is processed by Intercom under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data is processed. In no event will the terms of this DPA lessen Intercom's responsibilities or liabilities set forth in the Agreement, which includes Exhibit D (Terms Addendum).

1. **Definitions.** Any capitalized term used but not defined in this DPA has the meaning provided to it in the Agreement.
 - i. **"Account Data"** means Personal Data that relates to Customer's relationship with Intercom, including to access Customer's account and billing information, identity verification, maintain or improve performance of the Services, provide support, investigate and prevent system abuse, or fulfill legal obligations.
 - ii. **"Affiliate"** means any entity controlled by, controlling or under common control by an entity, where "control" means ownership of or the right to control greater than 50% of the voting securities of such entity.
 - iii. **"Applicable Data Protection Legislation"** refers to laws and regulations applicable to Intercom's processing of personal data under the Agreement, including but not limited to (a) the GDPR, (b) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2019 (together, "**UK Data Protection Laws**"), (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss DPA**"), (d) CCPA, and (e) Australian Privacy Principles and the Australian Privacy Act (1988), in each case, as may be amended, superseded or replaced.
 - iv. **"CCPA"** means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder, in each case, as may be amended from time to time.
 - v. **"Controller"** or **"controller"** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
 - vi. **"Customer Data"** means personal data that relates to Customer's relationship with Intercom, including Personal Data that Intercom processes as a Processor on behalf of Customer.
 - vii. **"Europe"** means for the purposes of this DPA the European Economic Area ("**EEA**"), United Kingdom ("**UK**") and Switzerland.
 - viii. **"GDPR"** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
 - ix. **"Personal Data"** or **"personal data"** means any information, including personal information, relating to an identified or identifiable natural person ("data subject") or as defined in and subject to Applicable Data Protection Legislation.
 - x. **"Privacy Policy"** means the then-current privacy policy for the Services available at <https://www.Intercom.com/legal/privacy>.
 - xi. **"Processor"** or **"processor"** means the entity which processes Personal Data on behalf of the Controller.
 - xii. **"Processing"** or **"processing"** (and **"Process"** or **"process"**) means any operation or set of operations performed upon Personal Data, whether or not by automated means, means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

- xiii. **"Restricted Transfer"** means: (i) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.
- xiv. **"Security Breach"** means a breach of security leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data transmitted, stored or otherwise processed by Intercom. A Security Incident shall not include an unsuccessful attempt or activity that does not compromise the security of Customer Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.
- xv. **"Standard Contractual Clauses" or "SCCs"** means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN> ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or (d) of the UK GDPR ("UK SCCs") and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs") (in each case, as updated, amended or superseded from time to time).
- xvi. **"Sub-processor" or "sub-processor"** means (a) Intercom, when Intercom is processing Customer Data and where Customer is itself a processor of such Customer Data, or (b) any third-party Processor engaged by Intercom or its Affiliates to assist in fulfilling Intercom's obligations under the Agreement and which processes Customer Data. Sub-processors may include third parties or Intercom Affiliates but shall exclude Intercom employees, contractors or consultants.
- xvii. **"Third Party Request"** means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

2. Applicability and Scope.

- i. **Applicability.** This DPA will apply only to the extent that Intercom processes, on behalf of Customer, Personal Data to which Applicable Data Protection Legislation applies.
- ii. **Scope.** The subject matter of the data processing is the provision of the Services, and the processing will be carried out for the duration of the Agreement. Schedule 1 (Details of Processing) sets out the nature and purpose of the processing, the types of Personal Data Intercom processes and the categories of data subjects whose Personal Data is processed.
- iii. **Intercom as a Processor.** The parties acknowledge and agree that regarding the processing of Customer Data, Customer may act either as a controller or processor and Intercom is a processor. Intercom will process Customer Data in accordance with Customer's instructions as set forth in Section 5 (Customer Instructions).
- iv. **Intercom as a Controller of Account Data.** The parties acknowledge that, regarding the processing of Account Data, Customer is a controller and Intercom is an independent controller, not a joint controller with Customer. Intercom will process Account Data as a controller (a) in order to manage the relationship with Customer; (b) carry out Intercom's core business operations; (c) in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) identity verification; (e) to comply with Intercom's legal or regulatory obligations; and (f) as otherwise permitted under Applicable Data Protection Legislation and in accordance with this DPA, the Agreement, and the Privacy Policy.

3. Intercom as a Processor – Processing Customer Data.

- i. Customer Instructions. Customer appoints Intercom as a processor to process Customer Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents, and detecting and preventing exploits or abuse); (b) as necessary to comply with applicable law, including Applicable Data Protection Legislation; and (c) as otherwise agreed in writing between the parties ("Permitted Purposes").
- ii. Lawfulness of Instructions. Customer will ensure that its instructions comply with Applicable Data Protection Legislation. Customer acknowledges that Intercom is neither responsible for determining which laws are applicable to Customer's business nor whether Intercom's Services meet or will meet the requirements of such laws. Customer will ensure that Intercom's processing of Customer Data, when done in accordance with Customer's instructions, will not cause Intercom to violate any applicable law, including Applicable Data Protection Legislation. Intercom will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate applicable law, including Applicable Data Protection Legislation.
- iii. Additional Instructions. Additional instructions outside the scope of the Agreement or this DPA will be mutually agreed to between the parties in writing.

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

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

6. Confidentiality.

- i. Confidentiality Obligations of Intercom Personnel.
 - a. Security Policy and Confidentiality. Intercom requires all employees to acknowledge in writing, at the time of hire, they will adhere to terms that are in accordance with Intercom's security policy and to protect Customer Data at all times. Intercom requires all employees to sign a confidentiality statement at the time of hire.
 - b. Intercom will ensure that any person that it authorizes to process Customer Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality (whether in accordance with Intercom's confidentiality obligations in the Agreement or a statutory duty, whichever duty is greater).
 - c. Background Checks. Intercom conducts at its expense a criminal background investigation on all employees who assist in the performance of the Agreement.
- ii. Responding to Third Party Requests. In the event any Third Party Request is made directly to Intercom in connection with Intercom's processing of Customer Data, Intercom will promptly inform Customer and provide details of the same, to the extent legally permitted. Intercom will not respond to any Third Party Request, without prior notice to Customer and an opportunity to object, except as legally required to do so or to confirm that such Third Party Request relates to Customer.

7. Sub-processors.

- i. Authorization for Sub-processing. Customer agrees that (a) Intercom may engage Sub-processors as listed at <https://www.intercom.com/legal/security-third-parties> (the "Sub-processor Page") which may be updated from time to time and Intercom Affiliates; and (b) such Affiliates and Sub-processors respectively may engage third party processors to process Customer Data on Intercom's behalf. Customer

provides a general authorization for Intercom to engage onward sub-processors that is conditioned on the following requirements: (a) Intercom will restrict the onward sub-processor's access to Customer Data only to what is strictly necessary to provide the Services, and Intercom will prohibit the sub-processor from processing the Personal Data for any other purpose. (b) Intercom agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation and said obligations shall be no less protective of Customer Data as the protections listed in this Agreement; and (c) Intercom will remain liable and accountable for any breach of this DPA or Agreement that is caused by an act or omission of its sub-processors.

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

- a. Customer understands that effective operation of the Services may require the transfer of Customer Data to Intercom Affiliates, such as Intercom, Inc., or to Intercom's Sub-processors, see Schedule 3. Customer hereby authorizes the transfer of Customer Data to locations outside Europe (Intercom's primary processing facilities are in the United States of America), including to Intercom Affiliates and Sub-processors, subject to continued compliance with this DPA throughout the duration of the Agreement. Customer hereby provides general authorization to Intercom engaging additional third-party Sub-processors to process Customer Data within the Services for the Permitted Purposes.
- b. Intercom may, by giving reasonable notice to the Customer, add to the Sub-processor Page. Intercom will notify Customer if it intends to add or replace Sub-processors from the Sub-Processor Page at least 10 days prior to any such changes. To receive such notification, Customers can follow link <http://privacy.intercom.com/third-party-subscribe> to join Intercom's distribution list. If Customer objects to the appointment of an additional Sub-processor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, then Intercom will work in good faith with Customer to find an alternative solution. In the event that the parties are unable to find such a solution, Customer may terminate the Agreement at no additional cost.

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

9. Security.

- i. Intercom has in place and will maintain throughout the term of this Agreement appropriate technical and organizational measures designed to protect Customer Data against Security Breaches.
- ii. These measures shall at a minimum comply with applicable law and include the measures identified in Schedule 2 (Technical and Organizational Security Measures).
- iii. Customer acknowledges that the security measures are subject to technical progress and development and that Intercom may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.
- iv. Intercom will ensure that any person authorized to process Customer Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality.
- v. Upon becoming aware of a Security Breach involving Customer Data processed by Intercom on behalf of Customer under this DPA, Intercom shall notify Customer without undue delay and shall provide such information as Customer may reasonably require, including to enable Customer to fulfil its data breach reporting obligations under Applicable Data Protection Legislation.
- vi. Intercom's notification of or response to a Security Breach shall not be construed as an acknowledgement by Intercom of any fault or liability with respect to the Security Breach.
- vii. Customer is solely responsible for its use of the Service, including (a) making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of Customer Data; (b) securing the

account authentication credentials, systems and devices Customer uses to access the Service; and (c) backing up Customer Data.

10. Reserved.

11. Audits.

- i. The parties acknowledge that when Intercom is acting as a processor on behalf of Customer, Customer must be able to assess Intercom's compliance with its obligations under Applicable Data Protection Legislation and this DPA.
- ii. Intercom shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and the obligations under Article 28 of the GDPR. While it is the parties' intention ordinarily to rely on the provision of the documentation to demonstrate Intercom's compliance with this DPA and the provisions of Article 28 of the GDPR, Intercom shall permit Customer (or its appointed third party auditors) to carry out an audit at Customer's cost and expense (including without limitation the costs and expenses of Intercom) of Intercom's processing of Customer Data under the Agreement following a Security Breach suffered by Intercom, or upon the instruction of a data protection authority acting pursuant to Applicable Data Protection Legislation. Customer must give Intercom reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Intercom's operations. Any such audit shall be subject to Intercom's security and confidentiality terms and guidelines and may only be performed a maximum of once annually. If Intercom declines to follow any instruction requested by Customer regarding audits, Customer is entitled to terminate the Agreement.
- iii. Intercom uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Data. A description of Intercom's certifications and standards for audit can be found at <https://www.Intercom.com/security>.

12. Transfer Mechanisms.

- i. Location of Processing. Customer acknowledges that Intercom and its Sub-processors may transfer and process personal data to and in the United States of America and other locations in which Intercom, its Affiliates or its Sub-processors maintain data processing operations, as more particularly described in the Sub-processor Page. Intercom shall ensure that such transfers are made in compliance with Applicable Data Protection Legislation, the Agreement, and this DPA.
- ii. Transfer Mechanism. The parties agree that when the transfer of personal data from Customer (as "data exporter") to Intercom (as "data importer") is a Restricted Transfer and Applicable Data Protection Legislation require that appropriate safeguards are put in place, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this DPA, as follows:
 - a. In relation to transfers of Customer Data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:
 1. Module Two or Module Three will apply (as applicable);
 2. in Clause 7, the optional docking clause will apply;
 3. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in section 7.ii.b of this DPA;
 4. in Clause 11, the optional language will not apply;
 5. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the EU Member State in which the data exporter is established and if no such law by Irish law;
 6. in Clause 18(b), disputes shall be resolved before the courts of the EU Member State in which the data exporter is established and otherwise Ireland;
 7. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and
 8. Subject to section 9.iii of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA;

- b. In relation to transfers of Account Data protected by the GDPR and processed in accordance with Section 2.iv of this DPA, the EU SCCs shall apply, completed as follows:
 1. Module One will apply;
 2. in Clause 7, the optional docking clause will apply;
 3. in Clause 11, the optional language will not apply;
 4. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
 5. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
 6. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and
 7. Subject to section 9.iii of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA;
- c. In relation to transfers of personal data protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under sub-paragraphs (a) and (b) above will apply with the following modifications:
 1. references to "Regulation (EU) 2016/679" shall be interpreted as references to UK Privacy Laws or the Swiss DPA (as applicable);
 2. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Privacy Laws or the Swiss DPA (as applicable);
 3. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);
 4. the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);
 5. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the UK Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);
 6. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);
 7. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and
 8. with respect to transfers to which UK Privacy Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.
- d. To the extent that and for so long as the EU SCCs as implemented in accordance with sub-paragraph (a)-(c) above cannot be used to lawfully transfer Customer Data and Account Data in accordance with the UK GDPR to Intercom, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Schedules 1 and 2 of this DPA.
- e. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

Customer agrees to this section ii only to the extent required by Applicable Data Protection Legislation.

- iii. Alternative Transfer Mechanism. To the extent that Intercom adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Applicable Data Protection Legislation) ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall upon notice to Customer and an opportunity to object, apply

instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Legislation applicable to Europe and extends to territories to which Customer Data and Account Data is transferred).

13. Cooperation and Data Subject Rights.

- i. Data Subject Rights. Intercom shall, taking into account the nature of the processing, provide reasonable assistance to Customer where possible and at Customer's cost and expense, to enable Customer to respond to requests from a data subject seeking to exercise their rights under Applicable Data Protection Legislation. In the event that such request is made directly to Intercom, if Intercom can, through reasonable means, identify the Customer as the controller of the Personal Data of a data subject, Intercom shall promptly inform Customer of the same
- ii. Cooperation. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Legislation or (b) any Third Party Request relating to the processing of Account Data or Customer Data conducted by the other party, such party will promptly inform the other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Legislation.

14. Miscellaneous.

- i. If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail only to the extent required to maintain compliance with Applicable Data Protection Legislation. In this instance, the order of precedence will be: (a) this DPA; (a) the Agreement; and (c) the Privacy Policy. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail only to the extent required to maintain compliance with Applicable Data Protection Legislation. In all other instances, the Agreement will prevail.
- ii. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.
- iii. In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.
- iv. In the event (and to the extent only) of a conflict (whether actual or perceived) among Applicable Data Protection Legislation, the parties (or relevant party as the case may be) shall comply with the more onerous requirement or standard.
- v. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Sections 2(iii) and 2 (iv), Intercom reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation. Intercom will provide at least 30 day advance written notice of any such change.
- vi. Except as amended by this DPA, the Agreement will remain in full force and effect.
- vii. Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that Intercom access to Customer Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

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

Signed on behalf of Customer

Company legal name:
State Board of Administration of Florida

Signed on behalf of Intercom

Intercom

Signed:

Signed:

Name:

Name:

Title:

Title:

Date:

Date:

Schedule 1

DETAILS OF PROCESSING

Annex I

A. LIST OF PARTIES

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

Name of Data exporter:	The party identified as the "Customer" in the Agreement and this DPA
Address:	As set forth in the Agreement
Contact person's name, position, and contact details:	As set forth in the Agreement
Activities relevant to the data transferred under these Clauses:	See Annex 1(B) below
Signature and date:	This Annex I shall automatically be deemed executed when the DPA is executed by Customer
Role (controller/processor):	Controller or Processor

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

Name:	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):	Processor

B. DESCRIPTION OF PROCESSING/ TRANSFER

Categories of Data Subjects whose personal data is transferred	Module One Customer's employees and individuals authorized by Customer to access Customer's Intercom account: Employees or contact persons of Customer's prospects, customers, business partners and vendors. Modules Two and Three Customer's end users: Prospects, customers, business partners and vendors of Customer (who are natural persons).
Categories of Personal Data transferred	Module One

	<p>Account Data which constitutes Personal Data, such as name and contact information as well as Customer billing address.</p>
	<p>Modules Two and Three Any Customer Data processed by Intercom in connection with the Services and which could constitute any type of Personal Data included in chats or messages, including, without limitation, username, password, email address, IP address as well as customer attribute data, website page view data, click data and social media information. Intercom acknowledges that Customer Data will include names, birthdates, and the last four digits of People's social security numbers. People may also, on his or her own accord, submit other unsolicited personal information via the chat feature.</p>
Sensitive data transferred (if applicable) and applied restrictions or safeguards	Intercom does not knowingly collect (and Customer shall not submit) any sensitive data or any special categories of data (as defined under Applicable Data Protection Legislation)
Frequency of the transfer	Continuous.
Nature and purpose(s) of the data transfer and Processing	<p>Module One Personal data contained in Account Data will be processed to manage the account, including to access Customer's account and billing information, for identity verification, to maintain or improve the performance of the Services, to provide support, to investigate and prevent system abuse, or to fulfill legal obligations.</p> <p>Modules Two and Three Personal Data contained in Customer Data will be subject to the following basic processing activities:</p> <p>Intercom provides a communication platform to facilitate interaction and engagement between the Customer and end users. This service will consist of providing a communication platform for the Customer to use in order to on-board and retain end users as well as analyze their use of the Customer's product and/or services.</p> <p>Intercom will process personal data as necessary to provide the Services under the Agreement. Intercom does not sell Customer's Personal Data or Customer end users' Personal Data and does not share such end users' Personal Data with third parties for compensation or for those third parties' own business interests.</p> <p>Additional details about Intercom's products and services can be found at https://www.intercom.com.</p>
Retention period (or, if not possible to determine, the criterion used to determine the period)	<p>Module One Intercom will process Account Data as long as required (a) to provide the Services to Customer; (b) for Intercom's lawful and legitimate business needs; or (c) in accordance with applicable law or regulation. Account Data will be stored in accordance with the Privacy Policy.</p> <p>Modules Two and Three Upon termination or expiry of this Agreement, Intercom will (at Customer's election) delete or return to Customer all</p>

	<p>Customer Data (including copies) in its possession or control as soon as reasonably practicable and within a maximum period of 30 days of termination or expiry of the Agreement, save that this requirement will not apply to the extent that Intercom is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Intercom will securely isolate and protect from any further processing, except to the extent required by applicable law.</p>
<p>For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing</p>	<p>Modules Two and Three only</p> <p>Intercom will restrict the onward sub-processor's access to Customer Data only to what is strictly necessary to provide the Services, and Intercom will prohibit the sub-processor from processing the Personal Data for any other purpose.</p> <p>Intercom imposes contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation.</p> <p>Intercom will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.</p>
<p>Identify the competent supervisory authority/ies in accordance with Clause 13</p>	<p>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.</p>

Schedule 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Annex II

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

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

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

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data	<ul style="list-style-type: none"> • All data sent to or from Intercom is encrypted in transit using TLS 1.2. • Customer Personal Data is encrypted at rest using 256-bit encryption, leveraging AWS' encryption framework's model C as described in https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf • All Intercom datastores used to process Customer data are configured and patched using commercially reasonable methods according to industry-recognized system-hardening standards. • See "Encryption" at https://www.intercom.com/security.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<ul style="list-style-type: none"> • Intercom has implemented a formal procedure for handling security events. When security events are detected, they are escalated to an emergency alias, relevant parties are paged, notified, and assembled to rapidly address the event. After a security event is contained and mitigated, relevant teams write up a post-mortem analysis, which is reviewed in person and distributed across the company and includes action items that will make the detection and prevention of a similar event easier in the future. • All Customer Data is permanently stored in the USA and is backed up for disaster recovery. • Intercom relies on Amazon Web Services (AWS), a reputable Infrastructure-As-A-Service provider. Intercom leverages their portfolio of globally redundant services to ensure Services run reliably. Intercom benefits from the ability to dynamically scale up, or completely re-provision its infrastructure resources on an as-needed basis, across multiple geographical areas, using the same vendor, tools, and APIs. Intercom's infrastructure scales up and down on demand as part of day-to-day operations and does so in response to any changes in our customers' needs. This includes not just compute resources, but storage and database resources, networking, security, and DNS. Every component in Intercom's infrastructure is designed and built for high availability. • Intercom's data security, high availability, and built-in redundancy are designed to ensure application availability and protect information from accidental loss or destruction. Intercom's Disaster Recovery plan incorporates geographic failover between its 3 U.S. data centers. Subscription Service restoration is within commercially reasonable efforts and is performed in conjunction with AWS' ability to provide

	<p>adequate infrastructure at the prevailing failover location. All of Intercom recovery and resilience mechanisms are tested regularly and processes are updated as required.</p> <ul style="list-style-type: none"> • Intercom operates a dedicated 24x7 on-call incident management function, ready to immediately respond to, and mitigate, any Customer impacting issues. This is supported by Intercom's broader internal Availability program which is dedicated to ensuring Intercom maintains their system availability. • Intercom has no direct reliance on specific office locations to sustain operations. All operational access to production resources can be exercised at any location on the Internet. Intercom leverages a range of best-of- breed technologies and other critical cloud tools to deliver uninterrupted remote work for all employees. • All Customer Data deleted by Intercom is deleted from AWS datastores in accordance with the NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitation December 18, 2014 (available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf). With respect to Customer Data encrypted in compliance with this security policy, this deletion may be done by permanently and securely deleting all copies of the keys used for encryption. • See "Back Ups and Monitoring" at www.intercom.com/security.
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	<ul style="list-style-type: none"> • See response for "<i>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</i>" above.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	<ul style="list-style-type: none"> • Intercom regularly tests their security systems and processes to ensure they meet the requirements of this security policy and ensures that the physical and environmental security controls are audited for SOC 2 Type II compliance, among other certifications. • Application Scans. Intercom performs periodic (but no less than once per month) application vulnerability scans. Vulnerabilities shall be remediated on a risk basis. • Third party penetration tests. Intercom 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. Intercom maintains a security bug bounty program, which gives independent security researchers a platform for testing and submitting vulnerability reports.
Measures for user and identification authorisation	<ul style="list-style-type: none"> • Single Sign-On (SSO) • Logical Access Controls. Intercom assigns a unique ID to each employee and leverages an Identity Provider to manage access to systems processing Customer Data. • All access to systems processing Customer Data is protected by Multi Factor Authentication (MFA). • Intercom restricts access to Customer Data to only those people with a "need-to-know" for a Permitted Purpose and following least privileges principles. • Intercom regularly reviews at least every 180 days the list of people and systems with access to Customer Data and removes accounts upon

	<p>termination of employment or a change in job status that results in employees no longer requiring access to Customer Data.</p> <ul style="list-style-type: none"> • Intercom 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 Customer Data and will require that all passwords and access credentials are kept confidential and not shared among personnel. • Password best practices implemented by Intercom’s Identity Provider. 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 • Intercom maintains and enforces “account lockout” by disabling accounts with access to Customer Data when an account exceeds more than ten (10) consecutive incorrect password attempts. • Intercom does not operate any internal corporate network. All access to Intercom resources is protected by strong passwords and MFA. • Intercom 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	<ul style="list-style-type: none"> • See “<i>Measures of pseudonymisation and encryption of personal data</i>” above. • See “Infrastructure” at www.intercom.com/legal/security-policy.
Measures for the protection of data during storage	<ul style="list-style-type: none"> • Intrusion Prevention. Intercom implements and maintains a working network firewall to protect data accessible via the Internet and will keep all Customer Data protected by the firewall at all times. • Intercom 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 Customer Data. • Security Awareness Training. Intercom requires annual security and privacy training for all employees with access to Customer Data. • Intercom 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) • See “Back Ups and Monitoring” and “Permissions and Authentication” at https://www.intercom.com/security.
Measures for ensuring physical security of locations at which personal data are processed	<ul style="list-style-type: none"> • Physical Access Control. Intercom’s services and data are hosted in AWS’ facilities in the USA and protected by AWS in accordance with their security protocols. • Access only to approved personnel. • All personnel who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege and are time-bound. Requests

	are reviewed and approved by authorized personnel, and access is revoked after the requested time expires.
Measures for ensuring events logging	<ul style="list-style-type: none"> • See “Measures for the protection of data during storage” above. • See https://www.intercom.com/help/en/articles/4667982-review-actions-taken-in-your-workspace-with-teammate-activity-logs.
Measures for ensuring system configuration, including default configuration	<ul style="list-style-type: none"> • Change and Configuration Management. Intercom uses continuous automation for application and operating systems deployment for new releases. Integration testing and unit testing are done upon every build with safeguards in place for availability and reliability. Intercom has a process for critical emergency fixes that can be deployed to Customers within minutes. As such Intercom can roll out security updates as required based on criticality. • Access Control Policy and Procedures • Change Management Procedures
Measures for internal IT and IT security governance and management	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • See https://www.intercom.com/security.
Measures for ensuring data minimisation	<ul style="list-style-type: none"> • 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, Intercom will (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control as soon as reasonably practicable and within a maximum period of 30 days of termination or expiry of the Agreement, save that this requirement will not apply to the extent that Intercom is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Intercom will securely isolate and protect from any further processing, except to the extent required by applicable law. • More information about how Intercom processes personal data is set forth in the Privacy Policy available at https://www.intercom.com/legal/privacy.
Measures for ensuring data quality	<ul style="list-style-type: none"> • Intercom has a process that allows data subjects to exercise their privacy rights (including a right to amend and update their Personal Data), as described in Intercom's Privacy Policy. • See “Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services” above.
Measures for ensuring limited data retention	<ul style="list-style-type: none"> • See “Measures for ensuring data minimization” above.
Measures for ensuring accountability	<ul style="list-style-type: none"> • Intercom has implemented data protection policies • Intercom follows a compliance by design approach

	<ul style="list-style-type: none"> • Intercom maintains documentation of your processing activities • Intercom has appointed a data protection officer • Intercom 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.	<ul style="list-style-type: none"> • Secure Disposal. Return or Deletion. Intercom will permanently and securely delete all live (online or network accessible) instances of the Customer Data within 15 days upon Customer’s in-app deletion request provided Customer makes it clear that they require 15 days deletion, otherwise within 90 days. • Archival Copies. When required by law to retain archival copies of Customer Data for tax or similar regulatory purposes, this archived Customer Data is stored as a “cold” or offline (i.e., not available for immediate or interactive use) backup stored in a physically secure facility. • Intercom has a process that allows data subjects to exercise their privacy rights (including a right to amend and update their Personal Data), as described in Intercom’s Privacy Policy.
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.	<ul style="list-style-type: none"> • Vendor & Services Providers. Prior to engaging new third-party service providers or vendors who will have access to Intercom Data, Intercom conducts a risk assessment of vendors’ data security practices. • Intercom will restrict the onward sub-processor’s access to Customer Data only to what is strictly necessary to provide the Services, and Intercom will prohibit the sub-processor from processing the Personal Data for any other purpose. • Intercom imposes contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation. • Intercom will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.

Schedule 3

LIST OF SUB-PROCESSORS

Annex III

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

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

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

EXHIBIT D

TERMS ADDENDUM

AGREEMENT TRANSPARENCY

Consistent with the Florida Transparency in Contracting Initiative, the SBA posts certain operational contracts on its website, and this Agreement, as redacted and attached hereto as Exhibit D-1, will be one of the agreements posted. With the exception of any information Intercom has specifically identified and redacted from this Agreement as set forth in Exhibit D-1, Intercom hereby agrees that the SBA is authorized to post this Agreement and a description of the contents of the Agreement on the SBA's website. In addition, the parties may from time to time during the term of the Agreement enter into one or more amendments or addenda to this Agreement. With the exception of any information Intercom has specifically identified and redacted from any such amendment or addenda at the time Intercom delivers an executed counterpart of such to the SBA, Intercom hereby agrees that the SBA is authorized to post any such amendment or addendum and a description of the contents thereof on the SBA's website. Intercom hereby understands, acknowledges and agrees that the redaction of any such information does not mean that such redacted information is protected from disclosure pursuant to a public records request under Chapter 119, Florida Statutes, or as otherwise required by law or a court or authority of competent jurisdiction.

CONFIDENTIAL INFORMATION

Intercom agrees to keep confidential any and all Customer Data it obtains in the course of providing the Services set forth in this Agreement except to the extent otherwise required to be disclosed in order to provide the Services or required by any applicable federal or state law provided that prior to any such disclosure pursuant to applicable law Intercom shall give the Customer prompt written notice, unless applicable law prohibits notification, and Intercom shall use all reasonable efforts, in good faith, to provide the Customer the opportunity to quash or abate such legal process or seek a protective order.

GOVERNING LAW; VENUE

This Agreement shall be governed by, construed under and interpreted in accordance with laws of the State of Florida without regard to conflict of law principles. Any proceedings to resolve disputes regarding or arising out of this Agreement shall be conducted in the state courts located in Leon County, Florida, and the parties hereby consent to the jurisdiction and venue of those courts.

PUBLIC RECORDS

Notwithstanding any provision in this agreement between the parties, Intercom acknowledges and agrees that the Customer is bound by the provisions of Chapter 119 (Public Records), Florida Statutes, and in the event of any conflict between Chapter 119, Florida Statutes, and the terms of this Agreement between the parties, the provisions and procedures of Chapter 119, Florida Statutes will prevail. To the extent applicable, Intercom shall comply with Chapter 119, Florida Statutes. In particular, Intercom shall:


- a. Keep and maintain public records required by the Customer in order to perform the services under the Agreement (however Customer Data will be maintained and deleted as specified in the Return/Destruction of Customer Data section below);
- b. Upon request from the Customer's custodian of public records, provide the Customer with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes or as otherwise provided by Florida law;
- c. Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the term of the Agreement and following completion of the Agreement if the Intercom does not transfer the records to the Customer; and
- d. Upon completion of the Agreement, transfer, at no cost, to the customer all public records in Intercom's possession (if so directed by the Customer) (such transfer to be accomplished by allowing Customer to access and download such public records) or keep and maintain public records required by the Customer to perform the service (this is accomplished as provided in Return/Destruction of Customer Data below which requires maintenance of records for thirty days following termination). If Intercom transfers all public records to the Customer upon completion of the Agreement, Intercom shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Intercom keeps and maintains public records upon completion of the Agreement (and for clarity, which shall be only as provided in this Agreement), the Intercom shall meet all applicable requirements for retaining public records. Intercom shall provide all records that are stored electronically to the Customer, upon request from the Customer's custodian of public records, in a format that is compatible with the information technology systems of the Customer.

**IF INTERCOM HAS QUESTIONS REGARDING THE APPLICATION OF
CHAPTER 119, FLORIDA STATUTES, TO INTERCOM'S DUTY TO
PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT,
CONTACT THE
CUSTODIAN OF THE PUBLIC RECORDS AT:**

**STATE BOARD OF ADMINISTRATION OF FLORIDA
POST OFFICE BOX 13300
TALLAHASSEE, FL 32317-3300
(850) 488-4406
CustomerAGREEMENTS_DL@CustomerFLA.COM**

E-VERIFY

Intercom shall register with and use the E-Verify system to verify the employment eligibility of newly hired employees performing services within the United States in accordance with Section 448.095, Florida Statutes. Intercom acknowledges that Customer is subject to and Intercom agrees to comply with Section 448.095, Florida Statutes, as amended from time to time, to the extent applicable.



NONDISCLOSURE

Customer Data shall be considered confidential and proprietary information to the extent permitted by Florida or other applicable law. Intercom shall hold Customer Data in confidence and shall not disclose Customer Data to any person or entity except as necessary to provide the Service or as otherwise authorized by the Customer or as required by law. For purposes of this Section 2, Data Security, "Customer Data" means the same as "Customer Data" as defined in the Agreement.

