



DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is made as of the Effective Date by and between Intercom R&D Unlimited Company ("**Intercom**"), and Customer, pursuant to the Master SaaS Subscription Agreement, the Subscription Terms of Service or other written or electronic agreement between the parties (as applicable) ("**Agreement**").

This DPA forms part of the Agreement and sets out the terms that apply when Personal Data is processed by Intercom as a Processor 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 are processed. Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1. Definitions

For the purposes of this DPA:

- a) "**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.
- b) "**Applicable Data Protection Legislation**" means as applicable, European Data Protection Legislation and the CCPA.
- c) "**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.
- d) "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;
- e) "**Customer Data**" means Personal Data that Intercom processes as a Processor on behalf of Customer.
- f) "**Effective Date**" means the last date of execution below.
- g) "**Europe**" means, for the purposes of this DPA, the European Economic Area (which comprises the member states of the European Union, Norway, Iceland and Liechtenstein), the United Kingdom and Switzerland.
- h) "**European Data Protection Legislation**" means (i) 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 ("**GDPR**"); and (ii) any applicable data protection laws of the United Kingdom (including the UK GDPR and the Data Protection Act 2018); as may be amended, superseded or replaced from time to time;
- i) "**Processor**" means an entity which processes Personal Data on behalf of the Controller;
- j) "**Personal Data**" means "personal data" or "personal information" as defined in and subject to Applicable Data Protection Legislation;
- k) "**Privacy Shield**" means the E.U.-US and Swiss-US Privacy Shield Frameworks, as operated by the U.S. Department of Commerce, as may be amended, superseded or replaced from time to time.
- l) "**Privacy Shield Principles**" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to Directive 95/46/EC, details of which can be found at www.privacyshield.gov/eu-us-framework.
- m) "**Standard Contractual Clauses**" means the Standard Contractual Clauses for processors as set out in the European Commission's Decision 2010/97/EU of 5 February 2010, in the form attached as Exhibit C.
- n) "**Sub-processor**" means any 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 and consultants.
- o) The terms "**personal data**", "**controller**", "**processor**" and "**processing**" shall have the meaning given to them in European Data Protection Legislation and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

2. **Applicability and scope of DPA.**

- 2.1. Applicability. This DPA will apply only to the extent that Intercom processes, on behalf of Customer, Personal Data to which European Data Protection Legislation applies and Personal Data pertaining to California residents. This DPA does not apply to Personal Data that Intercom processes as a Controller.
- 2.2. Scope. The subject matter of the data processing is the provision of the Services and the processing will be carried out for the duration of the Agreement. Exhibit A sets out the nature and purpose of the processing, the types of Personal Data Intercom processes and the categories of data subjects whose Personal Data is processed.

3. **Roles and responsibilities.**

- 3.1. Parties' Roles. To the extent that Intercom processes Customer Data subject to European Data Protection Legislation in the course of providing the Services, it will do so only as a Processor acting on behalf of Customer (as Controller) and in accordance with the requirements of the Agreement.
- 3.2. Instructions. The Agreement and this DPA set out Customer's complete documented instructions to Intercom in relation to the processing of Customer Data and any processing required outside of the scope of these instructions will require prior written agreement between the parties.
- 3.3. Purpose Limitation. If Intercom is required to process Customer Data for any other purpose by European Union or national law to which Intercom is subject, Intercom shall inform Customer of this requirement before the processing, except where otherwise required by such law.
- 3.4. 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.

4. **Security.**

- 4.1. Security. Intercom will have in place and maintain throughout the term of this Agreement appropriate technical and organizational measures designed to protect Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing (a "**Security Incident**"). These measures shall at a minimum comply with applicable law and include the measures identified in Exhibit B ("**Security Measures**"). 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.
- 4.2. 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 a contractual or a statutory duty).
- 4.3. Upon becoming aware of a Security Incident in respect of 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. Intercom's notification of or response to a Security Incident shall not be construed as an acknowledgement by Intercom of any fault or liability with respect to the Security Incident.
- 4.4. 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.

5. Subprocessing.

- 5.1. Subprocessing. Customer agrees that (a) Intercom may engage Intercom Affiliates and Sub-processors as listed at <https://www.intercom.com/terms-and-policies#security-third-parties> (the "**Sub-processor Page**") which may be updated from time to time; and (b) such Affiliates and Sub-processors respectively may engage third party processors to process Customer Data on Intercom's behalf.
- 5.2. Intercom shall (i) impose on such Sub-processors data protection obligations that protect Customer Data to the same or substantially similar standard provided for by this DPA, and at a minimum compliant with the requirements of European Data Protection Legislation; and (ii) remain liable for any breach of the DPA caused by a Sub-processor, but only to the same extent that Intercom would be liable if it had provided the services of the Sub-processor directly under the terms of this DPA.
- 5.3. 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 click [here](#) (or 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.

6. International transfers.

- 6.1. Location of Processing. 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, such as Amazon Web Services. Customer hereby authorizes the transfer of Customer Data to locations outside Europe, including to Intercom Affiliates and Sub-processors, subject to continued compliance with this Section 6 throughout the duration of the Agreement.
- 6.2. Transfer mechanism. To the extent Intercom processes (or causes to be processed) Customer Data that is protected by European Data Protection Legislation ("**European Data**") in a country that does not provide an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Legislation), Intercom agrees to abide by and process such European Data in accordance with the Standard Contractual Clauses, which are incorporated into and form a part of this DPA. The parties agree that (i) Customer provides Intercom R&D Unlimited Company with a mandate to enter into the Standard Contractual Clauses in its name and on its behalf; (ii) for the purposes of the descriptions in the Standard Contractual Clauses, Intercom, Inc. shall be the "data importer" and Intercom R&D Unlimited Company shall be the "data exporter"; (iii) Intercom R&D Unlimited Company remains fully and solely responsible and liable to Customer for the performance of the Standard Contractual Clauses by Intercom, Inc. and any instructions, claims or enquiries in relation to the Standard Contractual Clauses should be directed to Intercom R&D Unlimited Company; and (iv) 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 this Agreement the Standard Contractual Clauses shall prevail to the extent of such conflict.
- 6.3. Privacy Shield. Intercom, Inc. is self-certified to the Privacy Shield. Although Intercom does not rely on the Privacy Shield as a legal basis to transfer Personal Data in light of the judgment of the Court of Justice of the European Union in Case C-311/18, for so long as Intercom is self-certified to the Privacy Shield it shall continue to process European Data in compliance with the Privacy Shield Principles and notify Customer if it makes a determination that it can no longer meet its obligation to provide the level of protection as is required by the Privacy Shield Principles.
- 6.4. Alternative transfer arrangements. If Intercom adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to applicable European Data Protection Legislation) for the transfer of European Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Legislation and extends to the territories to which European Data is

transferred) and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to such Alternative Transfer Mechanism.

- 6.5. Transfers to the UK. For the avoidance of doubt, when the European Union law ceases to apply to the United Kingdom ("UK") upon the UK's withdrawal from the European Union, and until such time as UK is deemed to provide adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Legislation), then to the extent Intercom processes (or causes to be processed) any Customer Data protected by European Data Protection Legislation applicable to the EEA and Switzerland in the UK, Intercom shall process such Customer Data in compliance with the Standard Contractual Clauses or any applicable Alternative Transfer Mechanism as described above.

- 6.6. Disclosures. Each party acknowledges that the other party may disclose this DPA (including the Standard Contractual Clauses) and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, a European data protection authority, or any other US or European judicial or regulatory body upon their request.

7. Cooperation.

- 7.1. Intercom shall, to the extent required by European 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 European Data Protection Legislation in relation to Personal Data that is subject to European Data Protection Legislation.

8. Audit.

- 8.1. 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 Incident 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 this DPA and the Agreement.

9. Data subjects' rights.

- 9.1. Intercom shall, taking into account the nature of the processing, provide reasonable assistance to Customer insofar as this is 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.

10. Deletion / return of Personal Data.

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

11. CCPA.

- 11.1. For purposes of this Section 11, the terms “business,” “commercial purpose,” “sell” and “service provider” have the meanings given in the CCPA, and “personal information” shall mean Personal Data that constitutes “personal information” governed by the CCPA.
- 11.2. It is the parties’ intent that with respect to any personal information, Customer is a business and Intercom is a service provider. Intercom shall not (a) sell any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Service, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Service; or (c) retain, use or disclose the personal information outside of the direct business relationship between the parties. Intercom hereby certifies that it understands its obligations under this Section 11 and will comply with them.
- 11.3. The parties acknowledge and agree that Intercom’s provision of the Service encompasses, and that the parties’ business relationship contemplates, Intercom’s performance of its obligations and exercise of its rights under the Agreement.

12. Miscellaneous.

- 12.1. This DPA contains certain terms required by Intercom relating to data protection, privacy and security which has been updated to reflect certain requirements of Applicable Data Protection Legislation, where applicable. In the event (and to the extent only) of a conflict (whether actual or perceived) between the GDPR and the CCPA, the parties (or relevant party as the case may be) shall comply with the more onerous requirement or standard which shall, in the event of a dispute in that regard, be solely determined by Intercom.
- 12.2. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 3.1, Intercom reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation.
- 12.3. Except as amended by this DPA, the Agreement will remain in full force and effect.
- 12.4. If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail.
- 12.5. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.
- 12.6. Notwithstanding anything in the Agreement or any 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.

[Signature Page Follows]

Signed on behalf of Customer

Signed on behalf of Intercom

Company legal name:


Intercom R&D Unlimited Company

ADOPTOTECH D.O.O.

Signed:



Signed:

DocuSigned by:

365A417D311845A...

Name:

MARIO BUNTIC

Name:

Bobby Pinero

Title:

CEO

Title:

Sr Director Finance

Date:

21.9.2020.

Date:

8/13/2020

AdoptoTech d.o.o.
Z a g r e b
ul. Ljudevita Posavskog 34 A

Exhibit A – Data Processing Appendix

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is: Intercom R&D Limited Company, under a mandate from Customer

Data importer

The data importer is: Intercom, Inc.

Nature of Services

The Nature of Services are set out in the Agreement which describes the provision of services to the Customer.

Categories of data subjects

- Prospects, customers, business partners and vendors of Customer (who are natural persons);
- Employees or contact persons of Customer's prospects, customers, business partners and vendors;
- Customers' end-users authorized to use the Services.

Categories of data processed

The personal data processed concern the following categories of data:

Any Customer Data processed by Intercom in connection with the Services and which could constitute any type of personal data or personal information 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.

Special categories of data (if applicable)

Intercom does not knowingly collect (and Customer shall not submit) any special categories of data (as defined under European Data Protection Legislation).

Processing operations

The personal data processed will be subject to the following basic processing activities (please specify):

- Personal Data will be transferred from the Customer to Intercom for Intercom to provide a communication platform to facilitate interaction and engagement between the Customer and People.
- This service will consist of providing a communication platform for the Customer to use in order to on-board and retain People as well as analyze their use of the Customer's product and / or services.
- Additional details about Intercom's products and services can be found at www.intercom.com.

Exhibit B – Security Measures

During the Agreement Term, when processing Personal Data on behalf of Customer in connection with the Services, Intercom has implemented and shall maintain appropriate technical and organizational security measures for the processing of such data, including the measures specified in this Exhibit to the extent applicable to Intercom's processing of Personal Data.

1. **Intrusion Prevention.**

- (a) 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.
- (b) 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.
- (c) Intercom uses anti-malware software and keeps the anti-malware software up to date.

2. **Security Awareness Training.** Intercom requires annual security and privacy training for all employees with access to Customer Data.

3. **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.

4. **Logical Access Controls.**

- (a) Intercom assigns a unique ID to each employee and leverages an Identity Provider to manage access to systems processing Customer Data.
- (b) All access to systems processing Customer Data is protected by Multi Factor Authentication (MFA).
- (c) Intercom restricts access to Customer Data to only those people with a "need-to-know" for a Permitted Purpose and following least privileges principles.
- (d) Intercom regularly reviews at least every 180 days the list of people and systems with access to Customer Data and removes accounts upon termination of employment or a change in job status that results in employees no longer requiring access to Customer Data.
- (e) 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.
 - 1. 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
- (f) 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.
- (g) Intercom does not operate any internal corporate network. All access to Intercom resources is protected by strong passwords and MFA.
- (h) Intercom monitors their production systems and implements and maintains security controls and procedures designed to prevent, detect and respond to identified threats and risks.
- (i) 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).

5. **Human Resource Security.**

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

(b) 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 all Customer Data at all times. Intercom requires all employees to sign a confidentiality statement at the time of hire.

6. Disaster Recovery and Back-up Controls.

(a) All Customer Data is permanently stored in the USA and is backed up for disaster recovery.

(b) 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.

(c) 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 adequate infrastructure at the prevailing failover location. All of Intercom recovery and resilience mechanisms are tested regularly and processes are updated as required.

(d) 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.

(e) 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.

(f) 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.

7. Business Continuity and Security Incident Response Plan. 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.

8. Storage and Transmission Security.

(a) Customer data is stored in multi-tenant datastores.

(b) All data sent to or from Intercom is encrypted in transit using TLS 1.2.

(c) 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>

(d) All Intercom datastores used to process Customer data are configured and patched using commercially reasonable methods according to industry-recognized system-hardening standards.

9. Internal Audits.

(a) 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.

10. Secure Disposal.

(a) Return or Deletion. Intercom will permanently and securely delete all live (online or network accessible) instances of the Customer Data within 90 days upon Customer's in-app deletion request.

(b) 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.

11. Risk Identification & Assessment.

(a) Application Scans. Intercom performs periodic (but no less than once per month) application vulnerability scans. Vulnerabilities shall be remediated on a risk basis.

(b) 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.

(c) Bug bounty program. Intercom maintains a security bug bounty program, which gives independent security researchers a platform for testing and submitting vulnerability reports.

12. 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.

13. 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.

Exhibit C

2010 Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Intercom, Inc. (hereinafter "**data importer**")

and

Intercom R&D Unlimited Company, under a mandate from Customer (hereinafter the "**data exporter**")

each a "**party**"; together "**the parties**",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

Clause 1 **Definitions**

For the purposes of the Clauses:

- (a) '**personal data**', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) '**the data exporter**' means the controller who transfers the personal data;
- (c) '**the data importer**' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) '**the subprocessor**' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) '**the applicable data protection law**' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) '**technical and organisational security measures**' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority. 3

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The details of the transfer are specified in Exhibit A of the DPA.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The technical and organizational security measures implemented by the data importer are as described in Exhibit B of the DPA.

Appendix 3 to the Standard Contractual Clauses

The parties acknowledge that Clause 10 of the Clauses permits them to include additional business-related terms provided they do not contradict with the Clauses. Accordingly, this Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below.

Where a party complies with the commercial interpretations set out in this Annex, that party shall be deemed by the other party to have complied with its commitments under the Clauses. However, it is not the intention of either party that the commercial clauses below will have the effect of contradicting the Clauses.

For the purposes of this Appendix, "**DPA**" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated and "**Agreement**" shall have the meaning given to it in the DPA.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted by the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a) and 5(b): Suspension of data transfers and termination:

2. The parties acknowledge that for the purposes of Clause 5(a), data importer may process the personal data only on behalf of the data exporter and in compliance with its documented instructions as provided by the data exporter in the DPA and these Clauses.
3. The parties acknowledge that if data importer cannot, for whatever reason, provide compliance with Clause 5(a) and/or Clause 5(b), the data importer agrees to promptly inform the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the affected part of the Services.
4. If the data exporter intends to suspend the transfer of personal data and/or terminate the affected part of the Services, it shall endeavour to first provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**"). In addition, the data exporter and data importer shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards or other measures, if any, may be reasonably required to ensure the data importer's compliance with the Clauses and data exporter's compliance with applicable data protection law, in accordance with Section 3.4 of the DPA.
5. If after the Cure Period the data importer has not or cannot cure the non-compliance in accordance with paragraph (4) above then the data exporter may suspend and/or terminate the affected part of the Services in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination).

Clause 5(f): Audit:

6. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Clause 8 (Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

7. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
8. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
9. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

10. Any claims brought under or in connection with the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations of liability set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

11. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.
12. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Clause 5 (Subprocessing) of the DPA.