DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "Addendum") is made by and between Instabug, Inc., a company having its principal place of business at mobile communication software ("Company") and the counterparty agreeing to these terms ("Client").

This Addendum is incorporated into the Terms of Service ("Agreement") between the Company and the Client and applies in respect of the provision of the Services to the Client except that Annex A (EU Annex) to this Addendum applies only to such Processing of Client Personal Data governed by EU Data Protection Law and Annex B (California Annex) to this Addendum applies only to such Processing of Client Personal Data governed by the CCPA. This Addendum applies only to the extent the Client is a Controller of Client Personal Data and Company is a Processor of Client Personal Data. This Addendum shall be effective for the term of the Agreement.

1. Definitions

1.1. For the purposes of this Addendum:

1.1.1. **"Client Personal Data"** means the Personal Data described under Section 2 of this Addendum, in respect of which the Client is the Controller;

1.1.2. **"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;

1.1.3. **"Data Protection Legislation"** means all applicable legislation relating to data protection and privacy including, where applicable, GDPR and CCPA.

1.1.4. **"Data Subject"** means the individual to whom Personal Data relates;

1.1.5. **"GDPR"** means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and any national implementing laws in any Member State of the European Union, as amended from time to time.

1.1.6. **"Personal Data"** means any information relating to an identified or identifiable Data Subject;

1.1.7. **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

1.1.8. **"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms "process", "processes" and "processed" will be construed accordingly;

1.1.9. **"Processor"** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller; and

1.1.10. **"Standard Contractual Clauses"** means the agreement executed by and between the parties and attached hereto as Schedule 1 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses

for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

1.1.11. **"CCPA"** means the California Consumer Privacy Act of 2018, as amended from time to time.

1.2. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

2. Details of the Processing

2.1. **Categories of Data Subjects**. This Addendum applies to the Processing of Client Personal Data relating to customers or other end users of the Client who use the applications developed by the Client.

2.2. **Types of Personal Data.** Client Personal Data includes Data Subjects' email, name and IP address, and other Personal Data that Client may submit through or upload to the Company's systems the extent of which is determined and controlled by the Client in its sole discretion.

2.3. **Subject-Matter, Nature And Purpose of The Processing**. The subject-matter, nature and purpose of Processing of Personal Data by Company is the provision of the Services to the Client that involves the Processing of Client Personal Data, as set out into the Agreement and any applicable Statement of Work.

2.4. **Duration of The Processing**. Client Personal Data will be Processed for the duration specified in the Agreement until deletion as instructed by the Client under this Addendum.

3. Processing of Clients' Personal Data

3.1. The parties acknowledge and agree that Client is the Controller of Client Personal Data and the Company is the Processor of that data. Company will only Process Client Personal Data as a Processor on behalf of and in accordance with the Client's prior written instructions. Company is hereby instructed to Process Client Personal Data to the extent necessary to enable Company to provide the

Services in accordance with the Agreement. In case Processing is required by the Data Protection Legislation to which the Company is subject, the Company shall (i) promptly notify the Client of that legal requirement and/or of the inability to comply with any instructions before the relevant Processing, to the extent permitted by the Data Protection Legislation; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Client Personal Data) until such time as the Client issues new instructions with which Company is able to comply (and if this provision applies, Company will not be liable to the Client under the Agreement in respect of any inability to perform the Services until such time as the Client issues new instructions).

3.2. Client shall, in its use of the Services, Process Client Personal Data in accordance with the requirements of the Data Protection Legislation. For the avoidance of doubt, Client's instructions for the Processing of Client Personal Data shall comply with the Data Protection Legislation. Client shall ensure that Client has provided or will provide any necessary notices to Data Subjects, and has obtained or will obtain all necessary rights and consents (to the extent required) for Company to Process Client Personal Data in accordance with this Addendum.

3.3. The Client acknowledges that the Company is reliant on the Client for direction as to the extent to which Company is entitled to Process Client Personal Data on behalf of Client in performance of the Services. Consequently the Company will not be liable under the Agreement for any claim brought by a Data Subject arising from any action or omission by the Company, to the extent that such action or omission resulted directly from the Client's instructions or from Client's failure to comply with its obligations under the applicable Data Protection Legislation.

3.4. In connection with the performance of the Agreement, the Standard Contractual Clauses as attached to this Addendum as Schedule 1 will apply to Client Personal Data that is transferred outside the

European Economic Area (“EEA”), either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will cease to apply if Company has implemented an alternative recognized compliance mechanism for the lawful transfer of personal data outside the EEA pursuant to Article 46 of the GDPR, like certification to the Privacy Shield Framework, and has informed Client thereof and provided evidence of such alternative recognized compliance mechanism.

4. Confidentiality

4.1. Company will ensure that any person whom Company authorizes to Process Client Personal Data on its behalf is subject to confidentiality obligations in respect of that Client Personal Data.

Security Measures

4.1 Company will implement appropriate technical and organizational measures to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data (described under Appendix 2 to the Standard Contractual Clauses), including, as appropriate,

4.1.1 the pseudonymization of Client Personal Data,

4.1.2 ensuring the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services,

4.1.3 restoring the availability and access to Client Personal Data in a timely manner in the event of a physical or technical incident, and

4.1.4 regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing

5. Appointment of Sub-Processors

5.1. Client hereby grants general written authorization to Company to appoint sub-Processors to perform specific services on Company's behalf which may require such sub-Processors to Process Client Personal Data. For the avoidance of doubt, the above authorization constitutes Client's prior written consent to the sub-Processing by the Company for purposes of Clause 11 of the Standard Contractual Clauses. If Company engages a sub-Processor to Process any Client Personal Data, it will:

5.2. Inform Client of any intended changes concerning the addition or replacement of such sub-Processors and Client will have an opportunity to object to such changes on reasonable grounds within thirty (30) business days after being notified. If the parties are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party; and

5.3. Enter into a binding written agreement with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Company under this Addendum.

6. Assistance

6.1. Taking into account the nature of the Processing, Company shall assist the Client by appropriate technical and organizational measures, insofar as this is possible and to the extent Company is legally permitted to do, for the fulfillment of the Client's obligation to respond to Data Subjects' requests for the exercise of Data Subjects' rights under the Data Protection Legislation. Client shall be solely responsible for responding to such requests.

6.2. At the Client's request, Company will provide the Client with reasonable assistance to facilitate conducting data protection impact assessments and consultation with competent data protection authorities if the Client is required to do so under the Data Protection Legislation, in each case solely to the extent that such assistance is necessary and relates to the Processing by the Company of the Client Personal Data, taking into account the nature of the Processing and the information available to the Company.

6.3. Company will, at the Client's request, provide the Client with reasonable assistance as necessary for the fulfilment of the Client's obligation to implement appropriate security measures to protect Client Personal Data.

7. Personal Dara Breaches

7.1. Company will:

7.2. notify the Client without undue delay after it becomes aware of any Personal Data Breach affecting any Client Personal Data; and

7.3. at the Client's request, promptly provide the Client with all reasonable assistance necessary to enable the Client to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Client is required to do so under the Data Protection Legislation.

8. Deletion or Return of Client Personal Data

8.1. Upon termination or expiration of the Agreement, the Company will either delete or return (at the election of the Client) the Client Personal Data in its possession as set out in the Agreement within a reasonable timeframe.

9. Information

9.1. Company will provide the Client with all information necessary to enable the Client to demonstrate compliance with its obligations under the Data Protection Legislation, and allow for and contribute to audits, including inspections, conducted by the Client or an auditor mandated by the Client, to the extent that such information is within Company's control and Company is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party. Client shall give Company reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and take reasonable measures to prevent unnecessary disruption to Company's operations. Client will

be responsible for any fees charged by any auditor appointed by Client to execute any such audit.

10. Limitation of Liability

10.1. Each Party's liability towards the other Party under or in connection with this Addendum will be limited in accordance with the provisions of the Agreement.

Annex A – EU Annex

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

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

Instabug's Clients (the data **exporter**)

Instabug, Inc. (the data **importer**)

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 Appendix 1.

Clause 1 - Definitions

For the purposes of the Clauses:

1. '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;
2. the data exporter' means the controller who transfers the personal data;
3. '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;
4. 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;
5. '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;
6. 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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
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:

1. 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;

2. 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;
3. That the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
4. 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, unauthorized 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
5. That it will ensure compliance with the security measures;
6. 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;
7. 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;
8. 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;
9. 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
10. That it will ensure compliance with Clause 4(a) to (i).

Clause 5 – Obligations of the data importer

The data importer agrees and warrants:

1. 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;
2. 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;
3. That it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
4. That it will promptly notify the data exporter about:
   4.1. 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,
   4.2. Any accidental or unauthorised access, and
   4.3. Any request received directly from the data subjects without responding to that request unless it has been otherwise authorized to do so;
5. 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;
6. 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;

7. 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;
8. That, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
9. That the processing services by the subprocessor will be carried out in accordance with Clause 11;
10. 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 & 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:
   1.1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   1.2. 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

1. 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

1. 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 fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to

bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12- Obligation after the termination of personal data processing services

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

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.

Instabug Signature

Date

---25th March 2020-----

Costumer Signature

Firmato digitalmente da:GIUSEPPE VIRGONE
Ruolo:AMMINISTRATORE UNICO
Organizzazione:AGORÀ S.P.A./15376371009
Data:25/03/2020 14:24:38

Date

Appendix 1 – To the Standard Contractual Clauses

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

1. **Data exporter**
   The data exporter is the entity identified as "Client" in the Addendum.
2. **Data importer**
   The data importer is Instabug, Inc., identified as Company in the Addendum.
3. **Data subjects**
   The personal data transferred concern the following categories of data subjects (please specify): Data subjects are defined in Section 2.1of the Addendum.
4. **Categories of data**
   The personal data transferred concern the following categories of data (please specify): Categories of personal data are defined in Section 2.2 of the Addendum.
5. **Special categories of data (if appropriate)**
   The personal data transferred concern the following special categories of data (please specify): None.
6. **Processing operations**
   The personal data transferred will be subject to the following basic processing activities (please specify): The processing activities defined in Section 2 of the Addendum and in the Agreement.

Appendix 2 – To the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Technical and Organizational Security Measures

The data importer is committed to maintaining the privacy, confidentiality and security of personal data of the data exporter's personal data. The data importer uses industry best practices, technology and security measures to protect any and all personal data that is transferred to it and to secure its networks, data centers and servers. The security measures adopted by the data importer (and its subcontractors) include, without limitation:

The maintenance of physical, electronic and procedural measures to safeguard the confidentiality of personal data in compliance with applicable data protection, privacy and data security laws and regulations. These include, without limitation, restricting access by the data importer's personnel and subcontractors on a role-based, need to know basis, background checks on data importer personnel; The implementation and enforcement of corporate policies and standards relating to the protection of information and security, which are strictly enforced. Failure to adhere to these policies and the standards will result in disciplinary action, which can include dismissal; Adopting a multi-layered approach to information security controls, which enable the data importer to protect against security breach; Compliance with applicable laws, regulations and security standards applicable to information security; The employment of highly trained staff who have relevant and up to date knowledge of data protection and data security risk management practices; and Regular reviews and controls against compliance with the above mentioned technical and organizational security measures.

1. **Amazon Web Services for all data storage and processing**
   The data importer uses Amazon Web Services ("AWS") for processing and storing of data. Data on AWS is only accessible when the data exporter requests it. All AWS security and data privacy compliance can be reviewed at https://aws.amazon.com/compliance/programs/. The use of AWS provides the data importer with an industry-leading environment for the protection of its customers' data.
2. **Access Control**
   Data processing systems shall be prevented from being used without

authorization. All systems are protected by the use of personally identifiable access keys that are expired on employee change of role or departure from the organization.

3. **Change Control**
   Persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording.
4. **Data Forwarding**
   Personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities. As the systems are located in Amazon Web Services, the data importer has no direct access to any of the physical media on which the personal data is stored. AWS compliance with physical media protection standards can be viewed at https://aws.amazon.com/compliance/programs/.
5. **Order Control**
   Personal data processed on behalf of a data exporter are processed strictly in compliance with the data exporter's instructions. Data importer shall encrypt all personal data that it possesses, including electronic messages and attachments, strictly in compliance with the data exporter's instructions.
6. **Availability control**
   Data must be protected against accidental destruction or loss.
7. **Separation control**
   Data collected for different purposes can be processed separately.
8. **Personnel of data importer**
   Any personnel of data importer entrusted with processing data exporter's personal data have undertaken to comply with the principle of confidentiality in accordance with statutory law. The undertaking to confidentiality shall continue after the termination of the above-entitled activities. Prior to providing access to personal data, the data processor shall train its personnel concerning the implementation of, compliance

with and enforcement of, the data processor's security program and the handling of the personal data.

9. **Adequate alternative measures**
   The technical and organizational security measures are subject to technical progress and development, and data importer may implement adequate alternative measures. Any material changes to technical and organizational measures must be documented. Data importer must provide data exporter with reasonable information in order to support data exporter's reporting upon written request by the data exporter. Data importer will provide to data exporter any security assessments/certifications previously performed (and if data importer has not previously performed security assessments/certifications, it shall perform and provide such assessments/certifications at data exporter's request).

Annex B – California Annex

1. For purposes of this Annex B, the terms "business", "commercial purpose", "service provider", "sell" and "personal information" have the meanings given in the CCPA.
2. With respect to Client Personal Data, Instabug is a service provider under the CCPA.
3. The Company will not (a) sell Client Personal Data; (b) retain, use or disclose any Client Personal Data for any purpose other than for the specific purpose of providing the Services, including retaining, using or disclosing the Client Personal Data for a commercial purpose other than providing the Services; or (c) retain, use or disclose the Client Personal Data outside of the direct business relationship between the Company and the Client.
4. The parties acknowledge and agree that the Processing of Client Personal Data authorized by Client's instructions described in Section 3 of this Addendum is integral to and encompassed by the Company provision of the Services and the direct business relationship between the parties.

5. Notwithstanding anything in the Agreement or any Order Form entered in connection therewith, the parties acknowledge and agree that the Company's access to Client Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

The Simplest In-App Feedback and Bug Reporting for Mobile Apps

Get started for free in less than a minute (https://dashboard.instabug.com/signup)

Overview

How It Works (/how-it-works)
Platforms (/platforms)
Integrations(/integrations)
Documentation (https://docs.instabug.com)
Pricing (/pricing)
FAQ (/faq)

Book a Demo (https://instabug.com/enterprise)

Company

Customers (/customers)
Blog (https://instabug.com/blog/)
Ambassador Program (https://instabug.com/ambassador-program)
Jobs (/jobs)

Instabug For

Live Apps (/live-apps)
Beta Apps (/beta-apps)
Startups (/startups)
Product Managers(/product-managers)

Products

Bug Reporting (/bug-reporting)
Crash Reporting (/crash-reporting)
In-App Chat (/in-app-chat)
In-App Surveys (/in-app-surveys)
Feature Requests (/feature-requests)

From Our Blog (https://instabug.com/blog/)

What We Learned from Analyzing 100 Million Bugs
Essential Tools For React Native Development
Comparison Between Top Beta App Distribution Tools
Introducing Feature Request Management, Bug Analytics, and More

Connect with Instabug

Facebook: https://www.facebook.com/Instabug/
Twitter: https://twitter.com/instabug
LinkedIn: https://www.linkedin.com/company/instabug/
Stack Overflow: https://stackoverflow.com/questions/tagged/instabug
GitHub: https://github.com/instabug

Contact Us: (mailto:contactus@instabug.com)

Terms and Conditions Privacy Policy