Alloy Software. Inc
PO Box 355
East Hanover, NJ, 07936, USA
+1-973-661-9700

Alloy Software
Data Protection Agreement

This Data Protection Agreement ("Agreement" or "DPA") forms part of the Managed Software Hosting Agreement ("MSHA") or other written or electronic agreement between Alloy Software Inc. ("Alloy Software" or "Processor") and Customer (or "Controller") for the purchase of online services from Alloy Software (including associated Alloy Software offline and mobile components) identified as "Services" in the applicable agreement, and hereinafter defined as "Services", to reflect the parties' agreement with regard to the Processing of Personal Data.

Processor and Controller are individually referred to as "**Party**" and collectively as "**Parties**".

1 Definitions

"**Account Administrator**" shall mean the individual authorized by Controller to receive notices from Processor.

"Data Protection Laws" shall mean the data protection laws of the country in which Controller is established, including the GDPR, California Consumer Privacy Act, and any data protection laws applicable to Controller in connection with the MSA and/or Terms.

"**DP Losses**" means all liabilities, including:

a) costs (including legal costs);

b) claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (whether material or non-material, and including for emotional distress);

c) to the extent permitted by applicable law:

i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a data protection authority or any other relevant Regulatory Authority;

ii) compensation to a Data Subject ordered by a data protection authority to be paid by Processor;

iii) the costs of compliance with investigations by a data protection authority or any other relevant Regulatory Authority.

"GDPR" shall mean the 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.

"Personal Data" shall mean any information relating to an identified or identifiable natural person as defined by the General Data Protection Regulation of the European Union ("GDPR" EC-2016/679) that is Processed by Processor as part of providing the services to Controller as described in Exhibit 1.

"Standard Contractual Clauses/EU Standard Contractual Clauses" mean the standard contractual clauses set forth in Schedule 1 for the transfer of Personal Data from a Data Controller in the European Economic Area to Processors established in third countries in the form set out in the Annex of European Commission Decision 2010/87/EU, as amended by incorporating the description of the Personal Data to be transferred and the technical and organizational measures to be implemented as set out in the Appendix.

"Controller", **"Data Subject"**, **"Personal Data Breach"**, **"Processor"** and **"Process"** shall have the meaning given to them in the GDPR.

2 Scope of contract and Distribution of Responsibilities

2.1 The Parties agree that, for Processing Personal Data, the Parties shall be Controller and Processor.

2.2 Processor shall Process Personal Data only on behalf of Controller and at all times only in accordance with this Data Processing Agreement, especially the respective Exhibits.

2.3 Within the scope of the MSA and/or Terms, each Party shall be responsible for complying with its respective obligations as Controller and Processor under Data Protection Laws.

3 Processing Instructions

3.1 Processor will process Personal Data in accordance with Controller's instructions. This Data Processing Agreement contains Controller's initial instructions to Processor. The Parties agree that Controller may communicate any change in its initial instructions to the Processor by way of written notification to the Processor and that Processor shall abide by such instructions. The Processor shall maintain a secure, complete, accurate and up to date record of all such individual instructions.

3.2 For the avoidance of doubt, any instructions that would lead to processing outside the scope of this Data Processing Agreement (e.g., because a new Processing purpose is introduced) will

require a prior agreement between the Parties and, where applicable, shall be subject to the contract change procedure under the respective Agreement.

3.3 Where instructed by Controller, Processor shall correct, delete, or block Personal Data.

3.4 Processor shall promptly inform the Controller in writing if, in Processor's opinion, an instruction infringes Data Protection Laws, and provide an explanation of the reasons for its opinion in writing.

3.5 Processor shall not be liable for any DP Losses arising from or in connection with any processing made in accordance with Controller's instructions following Controller's receipt of any information provided by Processor in this Section 2.

4 Processor Personnel

Processor will restrict its personnel from Processing Personal Data without authorization. Processor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5 Disclosure to Third Parties; Data Subjects Rights

5.1 Processor will not disclose Personal Data to any third party (including any government agency, court, or law enforcement) except as set forth in this agreement or with written consent from Controller or as necessary to comply with applicable mandatory laws. If Processor is obliged to disclose Personal Data to a law enforcement agency or third party, Processor agrees to give Controller reasonable notice of the access request prior to granting such access, to allow Controller to seek a protective order or other appropriate remedies. If such notice is legally prohibited, Processor will take reasonable measures to protect the Personal Data from undue disclosure as if it were Processor's own confidential information being requested and shall inform Controller promptly as soon as possible if and when such legal prohibition ceases to apply.

5.2 In case Controller receives any request or communication from Data Subjects which relates to the Processing of Personal Data ("**Request**"), Processor shall provide the Controller with full cooperation, information and assistance ("**Assistance**") in relation to any such Request where instructed by Controller.

5.3 Where Processor receives a Request, Processor shall (i) not directly respond to such Request, (ii) forward the request to Controller within 3 (**three**) business days of identifying the Request as being related to the Controller and (iii) provide Assistance according to further instructions from Controller.

6 Technical and Organizational Measures ("TOMs")

6.1 Processor shall implement and maintain appropriate technical and organizational security measures to ensure that Personal Data is Processed according to this Data Processing Agreement,

to provide Assistance and to protect Personal Data against a Personal Data Breach. Such measures are set out in Exhibit 2 Appendix 2.

6.2 Processor shall document the implemented TOMs and shall provide Controller with such documentation upon request.

7 Assistance with Data Protection Impact Assessment

7.1 Where a Data Protection Impact Assessment ("**DPIA**") is required under applicable Data Protection Laws for the Processing of Personal Data, Processor shall provide upon request Controller with reasonable cooperation and assistance needed to fulfill Customer's obligation to carry out a DPIA related to Customer's use of the Services, to the extent that Customer does not otherwise have access to the relevant information and to the extent such information is available to Processor.

7.2 The Controller shall pay the Processor reasonable charges mutually agreed between the parties for providing the assistance in Section 8, to the extent that such assistance is not reasonably able to be accommodated within the normal provision of the Services.

8 Information Rights

Processor shall, in accordance with Data Protection Laws, make available to Controller on request in a timely manner such information as is necessary to demonstrate compliance by Processor with its obligations under Data Protection Laws.

9 Data Incident Management and Notification

In respect of Service Data incident Processor shall:

9.1 notify Controller of a Personal Data Breach involving Processor or a subcontractor without undue delay (but in no event later than 72 hours after becoming aware of the incident);

9.2 make reasonable efforts to identify the cause of such incident and take those steps as Processor deems necessary and reasonable in order to remediate the cause of the incident to the extent that it is within Processor's reasonable control.

9.3 provide reasonable information, cooperation, and assistance to Controller in relation to any action to be taken in response to a Personal Data Breach under Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and national data protection authorities.

The obligations contained in this Section 9 should not apply to Data Incidents that are caused by Customer or Customer's users.

10 Subprocessing

10.1 Controller consents to Processor engaging third party subprocessors as listed in Appendix 4 to process the Personal Data to fulfil its obligations under this Agreement provided that, Processor will provide at least fifteen (15) days' either an in-product notice or a notice by email to the Account administrator prior to the appointment or replacement of any subprocessor. Controller may object to Processor's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Processor will either not appoint or replace the subprocessor or, if this is not possible, Controller may suspend or terminate the Service(s) (without prejudice to any fees incurred by Controller prior to such suspension or termination).

10.2 Where Processor, with Controller's consent, subcontracts its obligations and rights under this Data Processing Agreement it shall do so only by way of a binding written contract with the subcontractor which imposes essentially the same obligations according to Art. 28 GDPR especially with regard to instructions and TOMs on the subcontractor as are imposed on Processor under this Data Processing Agreement.

10.3 Processor must ensure that he has carefully selected the subprocessor with particular regard for the suitability of the subcontractor's TOMs. Processor has entered a written agreement with each Sub-processor containing data protection obligations not less protective than those in the Agreement with respect to the protection of Service Data to the extent applicable to the nature of the Services provided by such Sub-processor.

10.4 Where the subcontractor fails to fulfil its data protection obligations under the subcontracting agreement, Processor shall remain fully liable to Controller for the fulfilment of its obligations under this Data Processing Agreement and for the performance of the subcontractor's obligations.

11 International Data Transfer

11.1 Data that Alloy Software processes for the Customer as a data processor may be stored in the EU or outside of the EU depending on the Alloy Software product. Alloy Software may also process certain data about Customer or its users as a data controller, including in countries outside of the EU, in accordance with Alloy Software's privacy statement available at https://www.alloysoftware.com/resources/privacy/

11.2 Where there is international transfer of Personal Data to Processor's Group Companies or to a country which is not a member state of the European Union, or in another signatory state of the European Economic Area Agreement **("EEA Countries")** or an international organization, the following applies unless explicitly agreed otherwise by the parties in an Appendix:

a) The Standard Contractual Clauses will apply to Personal Data originating from Controller (who, for the purposes of the Standard Contractual Clauses shall be deemed the "Data Exporter") that is processed by Processor (who, for the purposes of the Standard Contractual Clauses shall be deemed the "Data Importer") or by Processor's subcontractor outside of the European Economic Area. If there is any conflict between the Standard Contractual Clauses and this Data Processing Agreement, the Standard Contractual Clauses shall prevail.

b) At Controller's request, the Standard Contractual Clauses shall be replaced, and the Parties shall execute new standard contractual clauses for transfers to data processors in third countries adopted pursuant to Art. 46 (2) c) or d) GDPR.

c) If and as long as the country where Personal Data is transferred to a country which is subject to an adequacy decision according to Article 45 (3) GDPR, no Standard Contractual Clauses are required. Once the adequacy decision is repealed or suspended, a) and b) shall automatically apply.

12 Term and Termination

12.1 This Data Processing Agreement becomes effective upon signature. It shall continue to be in full force and effect as long as Processor is processing Personal Data according to Exhibit 1 and shall cease automatically thereafter.

12.2 The Controller may terminate the Data Processing Agreement as well as the MSA and/or Terms for cause, at any time upon reasonable notice or without notice, as selected by Controller, if the Processor is in material breach of the terms of this Data Processing Agreement.

12.3 Where amendments are required to ensure compliance of this Data Processing Agreements or an Appendix with Data Protection Laws, the Parties shall agree on such amendments upon request of Controller and, for the avoidance of doubt, with no additional costs to Controller. Where the parties are unable to agree upon such amendments, either party may terminate the MSA and/or Terms and this Data Processing Agreement with 90 days written notice to the other party.

13 Deletion or Return of Personal Data

Controller may export all Service Data prior to the termination of the Customer's Account. In any event, following the termination of the Customer's Account, subject to the MSA and/or Terms, Service Data will be retained for a period of 30 days ("**Data Retention Period**") from such termination within which Controller may contact Processor to export Service Data. Beyond such Data Retention Period, Processor reserves the right to delete all Service Data in the normal course of operation except as necessary to comply with Processor's legal obligations, maintain accurate financial and other records, resolve disputes, and enforce its agreements. Service Data cannot be recovered once it is deleted.

14 Miscellaneous

14.1 In case of any conflict, the provisions of this Data Processing Agreement shall take precedence over the provisions of any other agreement with Processor.

14.2 The limitation of liability stated in the MSA and/or Terms apply to the breach of the Data Processing Agreement.

14.3 No Party shall receive any remuneration for performing its obligations under this Data Processing Agreement except as explicitly set out herein or in another agreement.

14.4 Where this Data Processing Agreement requires a "written notice" such notice can also be communicated per email to the other Party. Notices shall be sent to the contact persons set out in Exhibit 1 VII.

14.5 Any supplementary agreements or amendments to this Data Processing Agreement must be made in writing and signed by both Parties.

14.6 Should individual provisions of this Data Processing Agreement become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this agreement.

Appendix 1 to the DPA

Subject Matter and Details of Data Processing

Data subjects

Data Subjects are those individuals to whom personal data relates to and are Users or End-Users who interact using the Service(s).

Categories of personal data

Categories of data refers to the personal data of Users and End-Users, contained in electronic data, text, messages or other materials, submitted to the Service(s) by Customer through Customer's Account in connection with Customer's use of the Service(s).

Subject-matter and nature of the processing

The personal data processed will be subject to the basic processing activities required for the provision of the Service(s) by Alloy Software to the Customer that involves the processing of personal data. Personal data will be subject to those processing activities as may be specified in the Terms and the DPA.

Purpose of the processing

Personal data will be processed for purposes of providing the Service(s) set out in a Form, as further instructed by Customer in its use of the Service(s), and otherwise agreed to in the Terms, this DPA and any applicable Form.

Duration of processing

Personal Data will be processed for the duration of the Terms.

Appendix 2 to the DPA

EU Standard Contractual Clauses (processors)

For the purposes of Article 46.3 of Regulation (EU) 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as “Controller” in the Data Processing Agreement

(the **“data exporter”**)

and

Alloy Software, Inc.

PO Box 355, East Hanover, New Jersey 07936, USA

(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:

(a) **'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'** and **'supervisory authority'** shall have the same meaning as in Regulation (EU) 2016/679;

(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 Regulation (EU) 2016/679;

(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 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 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 organizational 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, 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 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 Regulation (EU) 2016/679;

(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 organizational 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 unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 of 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.

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 3 to the DPA

Security Measures

This Appendix forms part of the DPA and must be completed and signed by the parties. By signing the signature page of the Data Processing Agreement, the parties will be deemed to have signed this Appendix 2.

Processor maintains and enforces various policies, standards and processes designed to secure personal data and other data to which Processor employees are provided access, and updates such policies, standards and processes from time to time consistent with industry standards. Following is a description of some of the technical and organizational measures implemented by Processor as of the date of signature:

1. General Security Procedures

1.1 Processor shall be responsible for establishing and maintaining an information security program that is designed to: (i) protect the security and confidentiality of Personal Data; (ii) protect against anticipated threats or hazards to the security or integrity of the Personal Data; (iii) protect against unauthorized access to or use of the Personal Data; (iv) ensure the proper disposal of Personal Data, as further defined herein; and, (v) ensure that all employees and subcontractors of Processor, if any, comply with all of the foregoing.

1.2 Processor shall conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls.

1.3 In the event of any apparent or actual theft, unauthorized use or disclosure of any Personal Data, Processor shall immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof, and without undue delay and within 72 hours following confirmation of any such event, provide Controller notice thereof, and such further information and assistance as may be reasonably requested. Upon Controller request, remediation actions and reasonable assurance of resolution of discovered issues shall be provided to Controller.

2. Network and Communications Security

2.1 Processor shall not access and will not permit unauthorized persons or entities to access Controller computing systems and/or networks without Controller's express written authorization and any such actual or attempted access shall be consistent with any such authorization.

2.2 Processor shall take appropriate measures to ensure that Processor's systems connecting to Controller's systems and anything provided to Controller through such systems does not contain any computer code, programs, mechanisms or programming devices designed to, or that would enable, the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment, in any manner, to the operation of Controller's systems.

2.3 Processor shall maintain technical and organizational measures for data protection including: (i) firewalls and threat detections systems to identify malicious connection attempts, to block spam, viruses and unauthorized intrusion; (ii) physical networking technology designed to resist attacks by malicious users or malicious code; and (iii) encrypted data in transit over public networks using industry standard protocols.

3. Personal Data Handling Procedures

3.1 Processor shall maintain authorization and authentication technologies and processes to ensure that only authorized persons access Personal Data, including: (i) granting access rights on the basis of the need-to-know-principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords that meet complexity, length and duration requirements; (iv) storing passwords in a manner that makes them undecipherable if used incorrectly or recovered in isolation; (v) encrypting, logging and auditing all access sessions to systems containing Personal Data; and (vi) instructing employees on safe administration methods when computers may be unattended such as use of password protected screen savers and session time limits.

3.2 Processor shall maintain logical controls to segregate Personal Data from other data, including the data of other customers.

3.3 Processor shall maintain measures to provide for separate processing of data for different purposes including: (i) provisioning Controller within its own application-level security domain, which creates logical separation and isolation of security principles between customers; and (ii) isolating test or development environments from live or production environments.

Appendix 4 to the DPA

Subprocessors

Amazon Web Services

Primary cloud infrastructure provider for Alloy Software, where all SaaS applications are hosted. Almost all data stored, processed and transmitted through Alloy Software products and services resides on Amazon Web Services data centers.

Google LLC - Firebase Cloud Messaging (FCM)

Firebase Cloud Messaging (FCM) is a remote notifications service from Google, that Alloy Software uses to send notifications relating to our Android Apps. These notifications relate to the user's accounts that is registered to the service subscriptions maintained by our Customers. Users have an option to turn-off, the notifications through the system settings in their Android device.

##