bugcrowd

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is incorporated into the Master Customer Agreement, or other similar master agreement relating to certain Services with Bugcrowd, Inc. (the "Agreement") between Customer and Bugcrowd, Inc. ("Bugcrowd"), to reflect the parties' agreement about Processing of Personal Data, when applicable, in accordance with the requirements of Data Protection Laws and Regulations. References to the Agreement will be construed as including without limitation this DPA.

1. Definitions. "Data Protection Laws and Regulations" means the regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement, including the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"); "Personal Data" means any information relating to an identified or identifiable natural person that is governed by the Data Protection Laws; "Data Subject" means an identified or identifiable natural person to whom the Personal Data relates; "Controller" means the entity that determines the purpose and means of the Processing of Personal Data; "Processor" means the entity that processes Personal Data on behalf of the Controller and "Process" or "Processing" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automatic 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.. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

2. Processing of Personal Data.

a. **Roles of the Parties**. Bugcrowd provides Customer with access to Bugcrowd's proprietary, web-based, vulnerability reporting and disclosure software-as-a-service platform (the "Platform") under the Agreement. In connection with the Platform, the parties anticipate that Bugcrowd may process Personal Data relating to Data Subjects in the European Economic Area, Switzerland and elsewhere. The parties agree that Customer is the Controller solely responsible for determining the purposes and means of the processing of Personal Data, and Bugcrowd is Customer's processor responsible for Processing certain Personal Data on behalf of the Controller. Bugcrowd shall only Process Personal Data only to the extent necessary pursuant to Customer's instructions and as set forth in the Agreement. Bugcrowd may engage sub-processors to Process Personal Data pursuant to the requirements set forth in Section 2e "Sub-Processors" below. Customer expressly acknowledges and agrees that the Security Researchers, as defined in the Agreement, are not sub-processors of Bugcrowd and are not bound by the terms of this DPA.

b. **Customer's Processing of Personal Data**. Customer is solely responsible for its compliance with the Data Protection Laws and Regulations, including without limitation the lawfulness of any transfer of Personal Data to Bugcrowd and Bugcrowd's Processing of Personal Data. For the avoidance of doubt, but not by way of limitation, Customer's instructions for the Processing of Personal Data must comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from Data Subjects. Customer takes full responsibility to keep the amount of Personal Data provided to Bugcrowd to the minimum necessary for the performance of the Services. Customer shall be solely responsible for establishing and maintaining any data processing registers or overview as required by any applicable law, including without limitation the Data Protection Laws and Regulations. Customer acknowledges and consents that certain business operations necessary for the fulfilment of Bugcrowd's services hereunder may have been transferred or will be transferred in the future to one or more dedicated Bugcrowd affiliates independently managing the provision of such Services.

c. **Model Clauses.** In addition to the parties' other duties and obligations hereunder, the parties hereby agree to comply with the Standard Contractual Clauses based on the Commission Decision C (2010)593 Standard Contractual Clauses (Data Processors) document set forth in Exhibit A attached hereto (the "Model Clauses") or any such clauses amending, replacing or superseding the Model Clauses by a European Commission decision or by a decision made by any other authorized body.

d. **Customer's Right to Issue Instructions**. Bugcrowd shall only Process Personal Data in accordance with Customer's instructions. Subject to the terms of this DPA and with mutual agreement of the parties, Customer may issue written instructions concerning the type, extent and procedure of Processing. Customer is responsible for ensuring that all individuals who provide written instructions to Bugcrowd are authorized by Customer to issue instructions to Bugcrowd. Customer's initial instructions for the Processing of Personal Data are defined by the Agreement, Appendix 1 to this DPA, and any applicable order form or Statement of Work regarding the software and Services. Any changes of the subject matter of Processing and of procedures shall be agreed upon by the parties in writing prior to becoming effective.

e. **Details of Processing**. The initial nature and purpose of the Processing, duration of the Processing,

categories of Data Subjects, and types of Personal Data are set forth on Appendix 1.

f. **Bugcrowd Sub-Processors.** Customer agrees that Bugcrowd may engage sub-processors to Process Personal Data in accordance with the DPA. A list of sub-processors including their addresses is available upon request. The parties agree that copies of the sub-processor agreements that Customer may request Bugcrowd to provide pursuant to Clause 5(i) of the Model Clauses may have all the commercial clauses or clauses unrelated to data processing, removed by Bugcrowd beforehand and, that such copies will be provided by Bugcrowd, in a manner to be determined in its discretion, only upon reasonable request by Customer. When engaging sub-processors, Bugcrowd shall enter into agreements with the sub-processors to bind them to obligations which are substantially similar or more stringent than those set out in this DPA. Customer will not directly communicate with Bugcrowd's sub-processors about the software or Services, unless agreed to by Bugcrowd in Bugcrowd's sole discretion. Bugcrowd will notify Customer in advance of any changes to sub-processors using regular communication means such as email, websites, and portals. If Customer reasonably objects to the addition of a new sub-processors (*e.g.*, such change causes Customer to be non-compliant with applicable with Data Protection Laws and Regulations), Customer shall notify Bugcrowd in writing of its specific objections within thirty (30) days of receiving such notification. If Customer does not object within such period, the addition of the new sub-processor and, if applicable, the accession to this DPA shall be considered accepted. If Customer does object to the addition of a new sub-processor and Bugcrowd cannot accommodate Customer's objection, Customer may terminate the Services and software in writing within sixty (60) days of receiving Bugcrowd's notification.

g. **Return or Deletion of Customer Personal Data**. Unless otherwise required by applicable Data Protection Laws and Regulations, Bugcrowd will destroy or return to Customer the Customer Personal Data upon termination or expiration of the Services within a reasonable period. Bugcrowd shall have no obligation to return Customer Personal Data to Customer if the Customer Personal Data is available to Customer.

3. Representations and Warranties. Customer represents, warrants, and covenants that (a) the Personal Data has been collected and transferred to Bugcrowd in accordance with the Data Protection Laws and Regulations; (b) prior to its transfer to Bugcrowd, the Personal Data has been maintained, retained, secured and protected in accordance with the Data Protection Laws and Regulations; (c) Customer will respond to inquiries from Data Subjects and from applicable regulatory authorities concerning the Processing of the Personal Data, and will alert Bugcrowd of any inquiries from Data Subjects or from applicable regulatory authorities that relate to Bugcrowd's Processing of the Personal Data; (d) prior to the collection of Personal Data, the Customer has obtained all necessary consents from a Data Subject for Bugcrowd's Processing of Personal Data in accordance with this DPA, including Processing of Personal Data; (e) Customer will make available a copy of this Agreement to any Data Subject or regulatory authorities as required by the Data Protection Laws and Regulations or upon the reasonable request of a Data Subject or a regulatory authority; (f) Customer shall be solely responsible and liable for its compliance with the Data Protection Laws and Regulations; and (g) Customer will only transfer and provide Bugcrowd with such Personal Data required and requested by Bugcrowd in writing to perform the Services.

4. Rights of Data Subjects. Bugcrowd shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of such Data Subject's Personal Data and, to the extent applicable, Bugcrowd shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Bugcrowd shall correct erroneous Personal Data as directed by Customer in writing or pursuant to a process mutually agreed to in writing by the parties. Customer shall use its best efforts to respond to and resolve promptly all requests from Data Subjects which Bugcrowd provides to Customer. If Data Protection Laws and Regulations require Bugcrowd to take any corrective actions without the involvement of Customer, Bugcrowd shall take such corrective actions and inform Customer. Customer shall be responsible for any reasonable costs arising from Bugcrowd's provision of such assistance under this Section. To the extent legally permitted, Customer shall be responsible for any costs arising from Bugcrowd's provision of such assistance.

5. Bugcrowd Personnel. Bugcrowd shall train personnel engaged in the Processing of Personal Data of the confidential nature of the Personal Data and provide appropriate training based on their responsibilities. Bugcrowd shall execute written agreements with its personnel to maintain the confidentiality of Personal Data, including post the termination of the personnel engagement. Bugcrowd shall use commercially reasonable efforts to limit access to Personal Data to personnel who require such access to perform the Agreement. If required by Data Protection Laws and Regulations, Bugcrowd shall appoint a data protection officer. Upon request, Bugcrowd will provide the contact details of the appointed person.

6. Security. Bugcrowd will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects. In assessing the appropriate level of security, Bugcrowd shall weigh the risks presented by

processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. In furtherance of the obligations described under this Section 6, Bugcrowd will take the security measures set forth in Appendix 2 of this DPA.

7. Audit.

a. **Audit Requests.** Subject to Section 7(c), upon Customer's written request, Bugcrowd will provide Customer with the most recent summary audit report(s) concerning the compliance and undertakings in this Agreement. Bugcrowd's policy is to share methodology, and executive summary information, not raw data or private information. Bugcrowd will reasonably cooperate with Customer by providing available additional information to help Customer better understand such compliance and undertakings. To the extent it is not possible to otherwise satisfy an audit obligation mandated by applicable Data Protection Laws and Regulations and subject to Section 7(c), only the legally mandated entity (such as a governmental regulatory agency having oversight of Customer's operations) may conduct an onsite visit of the facilities used to provide the Services. Unless mandated by Data Protection Laws and Regulations, no audits are allowed within a data center for security and compliance reasons. After conducting an audit under this Section 7 or after receiving an Bugcrowd report under this Section 7, Customer must notify Bugcrowd of the specific manner, if any, in which Bugcrowd does not comply with any of the security, confidentiality, or data protection obligations in this DPA, if applicable. Any such information will be deemed Confidential Information of Bugcrowd.

b. **Sub-Processors.** Customer may not audit Bugcrowd's sub-processors without Bugcrowd's and Bugcrowd's sub-processor's prior agreement. Customer agrees its requests to audit sub-processors may be satisfied by Bugcrowd or Bugcrowd's sub-processors presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Bugcrowd's data protection officer, the IT security department, data protection or quality auditors or other mutually agreed to third parties or certification by way of an IT security or data protection audit. Onsite audits at sub-processors premises may be performed by Bugcrowd acting on behalf of Controller.

c. **Audit Process.** Unless required by Data Protection Laws and Regulations, Customer may request a summary audit report(s) or audit Bugcrowd no more than once annually. Customer must provide at least four (4) weeks' prior written notice to Bugcrowd of a request for summary audit report(s) or request to audit. The scope of any audit will be limited to Bugcrowd's policies, procedures and controls relevant to the protection of Customer's Personal Data and defined in Appendix 1. Subject to Section 7(b), all audits will be conducted during normal business hours, at Bugcrowd's principal place of business or other Bugcrowd location(s) where Personal Data is accessed, processed or administered, and will not unreasonably interfere with Bugcrowd's day-to-day operations. An audit will be conducted at Customer's sole cost and by a mutually agreed upon third party who is engaged and paid by Customer, and is under a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement, obligating it to maintain the confidentiality of all Bugcrowd Confidential Information and all audit findings. Further, Customer agrees to pay the costs of any support provided by Bugcrowd (including internal resources) based on Bugcrowd's then-current rates. Before the commencement of any such on-site audit, Bugcrowd and Customer shall mutually agree upon the timing, and duration of the audit. Bugcrowd will reasonably cooperate with the audit, including providing auditor the right to review but not to copy Bugcrowd security information or materials during normal business hours. Customer shall, at no charge, provide to Bugcrowd a full copy of all findings of the audit. The results of the audit will be considered "Confidential Information" of Bugcrowd.

8. Limitation of Liability. To the extent permitted under law, each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Agreement and this DPA. For the avoidance of doubt, Bugcrowd's and its affiliates' total liability for all claims from the Customer arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and this DPA.

9. Governing Law. The parties agree that (1) governing law of this DPA, and (2) the forum for all disputes in respect of this DPA, shall be the same as set out in the Agreement, unless otherwise required by applicable Data Protection Laws and Regulations

Accepted and agreed:

CUSTOMER:

Signature:
Print Name:
Print Title:

BUGCROWD INC.:

Signature:
Print Name:
Print Title:

bugcrowd

Exhibit A
Model Clauses

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,

The Data Exporter and Data Importer listed in Appendix 1,
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 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 Exhibit A;

(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.

bugcrowd

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.

On behalf of DATA EXPORTER (Customer):

Signature:
Print Name:
Print Title:
Address:

On behalf of DATA IMPORTER (Bugcrowd, Inc.):

Signature:
Print Name:
Print Title:
Address: 921 Front Street, San Francisco, CA 94111

bugcrowd

Appendix 1
Processing Details and Instructions

Data Exporter: is the applicable "Customer" described in the DPA

Data Importer: is Bugcrowd, Inc., 921 Front Street, San Francisco, CA 94111. Email for notices is gc@bugcrowd.com

Data Subjects
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

1. Customers, prospects and business partners
2. Employees and their respective dependents, beneficiaries, and emergency contacts
3. Contractors (including contingent workers)
4. Volunteers, interns, temporary, and casual workers
5. Suppliers and vendors
6. Commercial representatives
7. Freelancers, agents, consultants, and other professional respondents, and their respective dependents, beneficiaries, and emergency contacts
8. Prospective employees and temporary staff
9. Advisors, consultants, and other professionals

Categories of Personal Data
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and may include, but is not limited to, the following categories of Personal Data:

1. First and last name
2. Business contact information
3. Personal contact information
4. Title, position, employer
5. ID data
6. Bank details
7. Transaction data
8. Connection data
9. Location data

Processing Operations
Bugcrowd is a provider of security testing and vulnerability reporting services, including through its Platform, which may process personal data upon the instruction of Customer in accordance with the terms of the DPA and the Agreement. Customer instructs Bugcrowd to Process Personal Data: (i) necessary for the provision of the Services; and (ii) as part of any Processing initiated by Customer.

Duration of Processing and Retention of Data
Bugcrowd will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing. Bugcrowd will retain Personal Data as long as required under law, unless otherwise agreed to in writing.

bugcrowd

Appendix 2
Security Measures

Bugcrowd will take, at a minimum, the security measures described in this Appendix 2 (or, as these measures are updated by Bugcrowd from time to time, measures that are of substantially similar stringency) in order to ensure compliance with such security provisions with regard to the Processing of Personal Data on behalf of Customer.

Access Control to Processing Areas
Bugcrowd implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data are processed or used. This is accomplished by:

- establishing security areas; 24 hours security service provided by property owner;
- protection and restriction of access paths;
- securing the data processing equipment;
- establishing access authorizations for staff and third parties, including the respective documentation;
- regulations on card-keys;
- restriction on card-keys;
- all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- the data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems
Bugcrowd implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- identification of the terminal and/or the terminal user to the Bugcrowd systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes;
- dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions;
- staff policies in respect of each staff access rights to personal data (if any), informing staff about their obligations and the consequences of any violations of such obligations, to ensure that staff will only access personal data and resources required to perform their job duties and training of staff on applicable privacy duties and liabilities;
- all access to data content is logged, monitored, and tracked; and
- use of state of the art encryption technologies.

Access Control to Use Specific Areas of Data Processing Systems
Bugcrowd commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- staff policies in respect of each staff member's access rights to the personal data;
- allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data and at least yearly monitoring and update of authorization profiles;
- release of data to only authorized persons;
- policies controlling the retention of backup copies; and
- use of state of the art encryption technologies.

Transmission Control
Bugcrowd implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data

travels;
- as far as possible, all data transmissions are logged, monitored and tracked; and
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

Input Control

Bugcrowd implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This is accomplished by:

- an authorization policy for the input of data into memory, as well as for the reading, alteration and deletion of stored data;
- authentication of the authorized personnel; individual authentication credentials such as user IDs that, once assigned, cannot be re-assigned to another person (including subsequently);
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of user codes (passwords) of at least eight characters or the system maximum permitted number and modification at first use and thereafter at least every 90 days in case of processing of sensitive data;
- following a policy according to which all staff of Bugcrowd who have access to personal data processed for Customers shall reset their passwords at a minimum once in a 180 day period;
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user ID's (requirement to re-enter password to use the relevant work station) that have not been used for a substantial period of time;
- automatic deactivation of user authentication credentials (such as user IDs) in case the person is disqualified from accessing personal data or in case of non use for a substantial period of time (at least six months), except for those authorized solely for technical management;
- proof established within Bugcrowd's organization of the input authorization; and
- electronic recording of entries.

Job Control

Bugcrowd ensures that personal data may only be processed in accordance with written instructions issued by Customer. This is accomplished by:

- binding policies and procedures for Bugcrowd's employees, subject to Customer's review and approval.

Bugcrowd ensures that if security measures are adopted through external entities it obtains written description of the activities performed that guarantees compliance of the measures adopted with this document. Bugcrowd further implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Bugcrowd and applicable laws; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to Customers upon request.

Availability Control

Bugcrowd implements suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy to ensure data access is restored within seven days and backup performed at least weekly;
- tape backup is stored off-site and available for restore in case of failure of SAN infrastructure for Database server;
- only the Customer(s) may authorize the recovery of backups (if any) or the movement of data outside of the location where the physical database is held, and security measures will be adopted to avoid loss or unauthorized access to data, when moved;
- regular check of all the implemented and herein described security measures at least every six months;
- backup tapes are only re-used if information previously contained is not intelligible and cannot be re-constructed by any

technical means; other removable media is destroyed or made unusable if not used; and
- any detected security incident is recorded, alongside the followed data recovery procedures, and the identification of the person who carried them out.

Separation of processing for different purposes

Bugcrowd implements suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:

- access to data is separated through application security for the appropriate users;
- modules within the Bugcrowd's data base separate which data is used for which purpose, i.e. by functionality and function; and
- at the database level, data is stored in different areas, separated per module or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Bugcrowd system administrators

Bugcrowd implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months;
- continuous audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Bugcrowd and applicable laws; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to Customer upon request.