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: (a) 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") and (b) the California Consumer Privacy Act of 2018 ("CCPA") and the California Privacy Rights Act of 2020 ("CPRA" together with the CCPA, the "California Privacy Laws"); "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. **Cross-Border Transfers of Personal Data**. Customer authorizes Bugcrowd and its sub-processors to transfer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

d. **Data Transfer Impact Assessment Questionnaire**. Bugcrowd agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire attached hereto as Exhibit A.

e. **EEA, Swiss, and UK Standard Contractual Clauses**. If Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Bugcrowd in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws and Regulations, the parties agree that the transfer shall be governed by the Standard Contractual Clauses attached hereto as Exhibit B. The parties agree that: (i) the certification of deletion

required by Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses will be provided upon Customer's written request; (ii) the measures Bugcrowd is required to take under Clause 8.6(c) of the Standard Contractual Clauses will only cover Bugcrowd's impacted systems; (iii) the audit described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 7 of this DPA; (iv) Bugcrowd may engage sub-processors using European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors or any other adequacy mechanism provided that such adequacy mechanism complies with applicable Data Protection Laws and Regulations and such use of sub-processors shall not be considered a breach of Clause 9 of the Standard Contractual Clauses; (v) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Standard Contractual Clauses will be limited to the termination of the Standard Contractual Clauses, in which case, the corresponding Processing of Personal Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (vi) unless otherwise stated by Bugcrowd, Customer will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Standard Contractual Clauses; (vii) the information required under Clause 15.1(c) will be provided upon Customer's written request; and (viii) notwithstanding anything to the contrary, Customer will reimburse Bugcrowd for all costs and expenses incurred by Bugcrowd in connection with the performance of Bugcrowd's obligations under Clause 15.1(b) and Clause 15.2 of the Standard Contractual Clauses without regard for any limitation of liability set forth in the Agreement. Each party's signature to this DPA shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

f. **Data Transfer Impact Assessment Questionnaire Outcome**. Taking into account the information and obligations set forth in this DPA and, as may be the case for a party, such party's independent research, to the parties' knowledge, the Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the attached Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws and Regulations is afforded a level of protection that is essentially equivalent to that guaranteed by applicable Data Protection Laws and Regulations.

g. **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, Exhibit C 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.

h. **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 Exhibit C.

i. **No Sale Of Personal Data**. Bugcrowd shall not sell any Customer Personal Data as the term "sell" is defined by the applicable California Privacy Laws. Bugcrowd shall not disclose or transfer any Customer Personal Data to a third party or other parties that would constitute "selling" as the term is defined by the applicable California Privacy Laws.

j. **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.

k. **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 Exhibit D 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 Exhibit C. 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:

Exhibit A

DATA TRANSFER IMPACT ASSESSMENT QUESTIONNAIRE

This Exhibit A forms part of the DPA. Capitalized terms not defined in this Exhibit A have the meaning set forth in the DPA.

1. What countries will Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.

    a. **Answer:** Personal Data may be stored in servers located in the United States and accessed via cloud-based applications.

2. What are the categories of data subjects whose Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** As set forth in Exhibit C.

3. What are the categories of Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** As set forth in Exhibit C.

4. Will any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures?

    a. **Answer:** Not to Bugcrowd's knowledge.

5. What business sector is Bugcrowd involved in?

    a. **Answer:** Bugcrowd provides a crowdsourced cybersecurity platform.

6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:**. Bugcrowd provides a crowdsourced cybersecurity platform, which may process data upon the instruction of Customer or for the purposes of fulfilling the obligations in and providing the services under the DPA, the Agreement and any Orders.

7. What is the frequency of the transfer of Personal Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Company Personal Data transferred on a one-off or continuous basis?

    a. **Answer:** Personal Data would be transferred on a one-off basis as described in question 6 above.

8. When Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to Bugcrowd, how is it transmitted to Bugcrowd? Is the Company Personal Data in plain text, pseudonymized, and/or encrypted?

    a. **Answer:** All Personal Data that is transmitted to Bugcrowd is protected in accordance with Exhibit D.

9. What is the period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?

    a. **Answer:** Bugcrowd will Process Personal Data for the duration of the Agreement and to enable enforcement and administration thereafter, unless otherwise agreed upon in writing. Bugcrowd will retain Personal Data for no longer than required under law, or for a shorter time as otherwise agreed to in writing.

10. Please list the Subprocessors that will have access to Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

Subprocessor	**Type of Data Processed**
Datadog	Browser client ip
	Login Activity
	Accidental PII
Mailgun	Email Address
Docusign	Tax Documents, NDA's etc
Outreach	Email Address
Drift	mixed
SFDC	Various Contact Details
Clari	Email Address
Marketo	Email Address
Personyze	Email Address
Gotowebinar	Email Address
Highspot	Email Address sometimes
Heap	IP
	Browsing history on-site
Google Analytics	IP
	Browsing history on-site
Tableau	Researchers#prime
Gainsight	email
	activities on platform
Google	email, document sharing, form response collection
AWS	Broad processing activities
Segment	email
	ip
	Browsing history on-site
Hellofax	Employee information over fax

11. Is Bugcrowd subject to FISA Section 702 or Executive Order 12333?

    a. **Answer:** As of the effective date of the DPA, no court has found Bugcrowd to be eligible to receive process issued under FISA Section 702 or Executive Order 12333, and no such court action is pending.

12. Has Bugcrowd ever received a request from public authorities for information about individuals located in the European Economic Area, Switzerland, and/or the United Kingdom pursuant to FISA Section 702 or Executive Order 12333? If yes, please explain.

a. **Answer:** No.

13. Has Bugcrowd ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

    a. **Answer:** No.

14. What safeguards will Bugcrowd apply during transmission and to the processing of Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws and Regulations?

    a. **Answer:** Those safeguards set forth in Exhibit D.

Exhibit B

This Exhibit B forms part of the DPA.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

(f) To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III).

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to

object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) Where the data exporter is established in an EU Member State, the following section applies: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. .....Name: Customer.

.....Address: As set forth in the Notices section of the Agreement.

.....Contact person's name, position and contact details: As set forth in the Notices section of the Agreement.

.....Activities relevant to the data transferred under these Clauses: As set forth in Exhibit A.

.....Role (controller/processor): Controller.

Data importer(s):

1.....Name: Bugcrowd.

.....Address: As set forth in the Notices section of the Agreement.

.....Contact person's name, position and contact details: As set forth in the Notices section of the Agreement.

.....Activities relevant to the data transferred under these Clauses: As set forth in Exhibit A.

.....Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

.....As set forth in Exhibit A.

Categories of personal data transferred

.....As set forth in Exhibit A.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....As set forth in Exhibit A.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....As set forth in Exhibit A.

Nature of the processing

.....As set forth in Exhibit A.

Purpose(s) of the data transfer and further processing

.....As set forth in Exhibit A.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

.....As set forth in Exhibit A.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....As set forth in Exhibit A.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

.....The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer shall implement and maintain appropriate technical and organisational measures designed to protect personal data in accordance with the DPA.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the DPA.

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This UK Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The effective date of the DPA.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Customer. Main address (if a company registered address): As set forth in the Notices section of the Agreement.	Full legal name: Bugcrowd. Main address (if a company registered address): As set forth in the Notices section of the Agreement.
Key Contact	Contact details including email: As set forth in the Notices section of the Agreement.	Contact details including email: As set forth in the Notices section of the Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	[x] The version of the Approved EU SCCs which this UK Addendum is appended to, detailed below, including the Appendix Information: Date: The effective date of the DPA.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties: As set forth in Exhibit B, Annex I.
Annex 1B: Description of Transfer: As set forth in Exhibit B, Annex I.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Exhibit B, Annex II.

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	Which Parties may end this UK Addendum as set out in Section 19: Importer.

Part 2: Mandatory Clauses

Entering into this UK Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Addendum	This International Data Transfer Addendum which is made up of this UK Addendum incorporating the Addendum EU SCCs.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the UK Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.

7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the UK Addendum EU SCCs (as applicable), the Approved UK Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this UK Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This UK Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this UK Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this UK Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

    l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this UK Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved UK Addendum which:

    a. makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18, if any Party selected in Table 4 "Ending the UK Addendum when the Approved UK Addendum changes", will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the UK Addendum; and/or

    b. its risk under the UK Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved UK Addendum.

20. The Parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved UK Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Exhibit C
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.

Exhibit D
Security Measures

Bugcrowd will take, at a minimum, the security measures described in this Exhibit D (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.