bugcrowd

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the master services agreement or other overarching agreement (i.e. consulting agreement, vendor agreement, subscription agreement, etc.) (the "**Agreement**") between Bugcrowd, Inc., its subsidiaries and other affiliated entities ("**Company**") and the entity listed and that signs as "**Service Provider**" on the signature page of this Agreement (Service Provider, together with Bugcrowd, are collectively referred to as the "**Parties**").

1. Subject Matter and Duration.

a) **Subject Matter.** This Addendum reflects the Parties' commitment to abide by Data Protection Laws concerning the Processing of Company Personal Data in connection with Service Provider's execution of the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

b) **Duration and Survival.** This Addendum will become legally binding upon the effective date of the Agreement or upon the date that the Parties sign this Addendum if it is completed after the effective date of the Agreement. Service Provider will Process Company Personal Data until the relationship terminates as specified in the Agreement. Service Provider's obligations and Company's rights under this Addendum will continue in effect so long as Service Provider Processes Company Personal Data.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Company Personal Data**" means Personal Data Processed by Service Provider on behalf of Company. The Company Personal Data and the specific uses of the Company Personal Data are detailed in **Exhibit A** attached hereto.

b) "**Data Protection Laws**" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Company Personal Data are subject. "Data Protection Laws" shall include, but not be limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"), the California Privacy Rights Act of 2020 ("**CPRA**") once in effect (the CCPA and CPRA are referred to collectively as the "**California Privacy Laws**"), and the EU General Data Protection Regulation 2016/679 ("**GDPR**").

c) "**Personal Data**" shall have the meaning assigned to the terms "personal data" and/or "personal information" under Data Protection Laws and shall, at a minimum, include any information relating to an identified or identifiable natural person.

d) "**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 automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

e) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Personal Data.

f) "**Services**" means any and all services that Service Provider performs under the Agreement.

g) "**Third Party(ies)**" means Service Provider's authorized contractors, agents, vendors and third party service providers (i.e., sub-processors) that Process Company Personal Data.

3. Data Use and Processing.

a) Documented Instructions. Service Provider and its Third Parties shall Process Company Personal Data solely for the purpose of providing the Services to Company, and solely to the extent necessary to provide the Services to Company, in each case, in accordance with the Agreement, this Addendum and Data Protection Laws. Service Provider will, unless legally prohibited from doing so, inform Company in writing if it reasonably believes that there is a conflict between Company's instructions and applicable law or otherwise seeks to Process Company Personal Data in a manner that is inconsistent with Company's instructions.

b) Authorization to Use Third Parties. To the extent necessary to fulfill Service Provider's contractual obligations under the Agreement or any Statement of Work, Company hereby authorizes (i) Service Provider to engage Third Parties and (ii) Third Parties to engage sub-processors.

c) Service Provider and Third Party Compliance. Service Provider shall (i) enter into a written agreement with Third Parties that imposes on such Third Parties (and their sub-processors) data

protection and security requirements for Company Personal Data that are at least as restrictive as the obligations in this Addendum; and (ii) remain responsible to Company for Service Provider's Third Parties' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Company Personal Data. Service Provider shall flow down all obligations in this Addendum to Third Parties (and their sub-processors) regarding, among other things: (i) Company Personal Data and (ii) all Company's and Company's regulator's rights regarding review and audit (including Company's right to appoint an independent third party to perform such review or audits).

d) Right to Object to Third Parties. Service Provider shall make available to Company a list of Third Parties that Process Company Personal Data upon reasonable request. Prior to engaging any new Third Parties that Process Company Personal Data, Service Provider will notify Company via email and allow Company thirty (30) days to object. If Company has legitimate objections to the appointment of any new Third Party, the Parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Company may terminate the part of the Service performed under the Agreement that cannot be performed by Service Provider without use of the objectionable Third Party. Service Provider shall refund any pre-paid fees to Company in respect of the terminated part of the Service.

e) Confidentiality. Any person or Third Party authorized to Process Company Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

f) Personal Data Inquiries and Requests. Service Provider agrees to provide reasonable assistance and comply with all reasonable instructions from Company related to any requests from individuals exercising their rights in Company Personal Data granted to them under Data Protection Laws (e.g., access, rectification, erasure, data portability, etc.). If a request is sent directly to Service Provider, Service Provider shall promptly notify Company within five (5) days of receiving such request and shall not respond to the request unless Company has authorized Service Provider to do so.

g) Sale of Company Personal Data Prohibited. Service Provider shall not sell Company Personal Data as the term "sell" is defined by the applicable California Privacy Laws. Service Provider shall not disclose or transfer Company Personal Data to a Third Party or other parties that would constitute "selling" as the term is defined by the applicable California Privacy Laws.

h) Data Protection Impact Assessment and Prior Consultation. Service Provider agrees to provide reasonable assistance at Company's expense to Company where, in Company's judgement, the type of Processing performed by Service Provider requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

i) Demonstrable Compliance. Service Provider agrees to keep records of its Processing in compliance with Data Protection Laws and provide any necessary records to Company to demonstrate compliance with this Addendum upon reasonable request.

4. Cross-Border Transfers of Personal Data.

a) Cross-Border Transfers of Personal Data. Company authorizes Service Provider and its Third Parties to transfer Company Personal Data across international borders, including from the European Economic Area to the United States. Where required, cross-border transfers of Company Personal Data must be supported by an approved adequacy mechanism.

b) Standard Contractual Clauses. Company and Service Provider will use the Standard Contractual Clauses in **Exhibit B** as the adequacy mechanism supporting the transfer and Processing of Company Personal Data. Each party's signature to this Addendum shall be considered a signature to the Standard Contractual Clauses.

5. Information Security Program.

a) Service Provider agrees to implement and maintain appropriate technical and organizational measures to protect Company Personal Data (the "**Information Security Program**"). At a minimum, such measures shall include:

i) Pseudonymisation of Company Personal Data where appropriate, and encryption of Company Personal Data in transit and at rest;

ii) The ability to ensure the ongoing confidentiality, integrity, availability of Service Provider's Processing and Company Personal Data;

iii) The ability to restore the availability and access to Company Personal Data in the event of a physical or technical incident;

iv) A process for regularly evaluating and testing the effectiveness of the Service Provider's Information Security Program to ensure the

security of Company Personal Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

6. Security Incidents.

a) Security Incident Procedure. Service Provider will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Company Personal Data in a timely manner.

b) Notice. Service Provider agrees to provide prompt written notice without undue delay (but in no event longer than twenty-four (24) hours) to Company's Designated POC if it knows or reasonably suspects that a Security Incident has taken place. Such notice will include all available details required under Data Protection Laws for Company to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

c) Remediation. Company has the right to participate in the investigation and response to the Security Incident and Service Provider agrees to cooperate fully in the investigation and remediation of any harm or potential harm caused by the Security Incident. To the extent that a Security Incident gives rise to a need, in Company's sole judgment to: (i) provide notification to public and/or regulatory authorities, individuals, or other persons, or (ii) undertake other remedial measures (including, without limitation, notice, credit monitoring services and the establishment of a call center to respond to inquiries – collectively, "**Remedial Action**"), at Company's request and direction, and at Service Provider's cost, Service Provider agrees to undertake such Remedial Actions. Company shall have sole discretion to control and direct the timing, content and manner of any notices, including but not limited to communication with Company customers and/or employees, regarding the same. If Company chooses to carry out the Remedial Action itself, Service Provider agrees to reimburse Company for its costs.

7. Audits.

a) Right to Audit; Permitted Audits. In addition to any other audit rights described in the Agreement, Company and its regulators shall have the right to an on-site audit of Service Provider's architecture, systems, policies and procedures relevant to the security and integrity of Company Personal Data, or as otherwise required by a governmental regulator:

i) Following any notice from Service Provider to Company of an actual or reasonably suspected Security Incident involving Company Personal Data;

ii) Upon Company's reasonable belief that Service Provider is not in compliance with Data Protection Laws, this Addendum or its security policies and procedures under the Agreement;

iii) As required by governmental regulators; and

iv) For compliance purposes, once annually.

b) Audit Terms. Any audits described in this Section shall be:

i) Conducted by Company or its regulator, or through a third party independent contractor selected by one of these parties;

ii) Conducted during reasonable times;

iii) To the extent possible, conducted upon reasonable advance notice to Service Provider; and

iv) Of reasonable duration and shall not unreasonably interfere with Service Provider's day-to-day operations.

c) Third Parties. In the event that Company conducts an audit through a third party independent auditor or a third party accompanies Company or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Service Provider's and Service Provider's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

d) Audit Results. Upon Service Provider's request, after conducting an audit, Company shall notify Service Provider of the manner in which Service Provider does not comply with any of the applicable security, confidentiality or privacy obligations or Data Protection Laws herein. Upon such notice, Service Provider shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Company when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Company may conduct a follow-up audit within six (6) months of Service Provider's notice of completion of any necessary changes. To the extent that a Service Provider audit and/or Company audit identifies any material security vulnerabilities, Service Provider shall remediate those vulnerabilities within fifteen (15)

days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

8. Data Storage and Deletion.

a) Data Storage. Service Provider will abide by the following with respect to storage of Company Personal Data:

i) Service Provider will not store or retain any Company Personal Data except as necessary to perform the Services under the Agreement.

b) Data Deletion. Service Provider will abide by the following with respect to deletion of Company Personal Data:

i) Within thirty (30) calendar days of the Agreement's expiration or termination, or sooner if requested by Company, Service Provider will securely destroy (per subsection (iii) below) all copies of Company Personal Data (including automatically created archival copies).

ii) Upon Company's request, Service Provider will promptly return to Company a copy of all Company Personal Data within thirty (30) days and, if Company also requests deletion of the Company Personal Data, will carry that out as set forth above.

iii) Company Personal Data shall be disposed of in a method that prevents any recovery of the data in accordance with industry best practices for shredding of physical documents and wiping of electronic media (e.g., NIST SP 800-88).

iv) Upon Company's request, Service Provider will provide a "Certificate of Deletion" certifying that Service Provider has deleted all Company Personal Data. Service Provider will provide the "Certificate of Deletion" within thirty (30) days of Company's request.

9. Indemnification.

a) Service Provider shall indemnify, defend, and hold harmless Company and its officers, directors, employees and agents from and against any claims, disputes, demands, liabilities, damages, losses, fines, and costs and expenses, including, without limitation, reasonable attorneys' fees arising out of or relating to: (i) a Security Incident; (ii) Service Provider's negligence or willful misconduct related to Company Personal Data; and/or (iii) Service Provider's breach of this Addendum.

10. Contact Information.

a) Company and Service Provider agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

- Company Designated POC:_____
  _____
- Service Provider Designated POC: _____
  _____

BUGCROWD, INC.

Signature: _____
Printed Name: _____
Title: _____
Date: _____

SERVICE PROVIDER
Entity Name: _____

Signature: _____
Printed Name: _____
Title: _____
Date: _____

bugcrowd

Exhibit A

1.1 Subject Matter of Processing	The Processing will involve Processing for: The subject matter of Processing is the Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	Includes the following: Data subjects whose Company Personal Data is Processed pursuant to the Agreement.
1.4 Nature and Purpose of Processing	Includes the following: The purpose of Processing of Company Personal Data by Service Provider is the performance of the Services pursuant to the Agreement.
1.5 Types of Personal Information	Includes the following: Company Personal Data Processed pursuant to the Agreement.

bugcrowd

Exhibit B

Standard Contractual Clauses (Processors)

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

Name of the data exporting organisation: Company (as defined in the Addendum).

.....

(the data **exporter**)

And

Name of the data importing organisation: Service Provider (as defined in the Addendum).

(the data **importer**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

bugcrowd

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.

bugcrowd

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is: Company.

Data importer
The data importer is: Service Provider.

Data subjects
The personal data transferred concern the following categories of data subjects: As set forth in Exhibit A.

Categories of data
The personal data transferred concern the following categories of data: As set forth in Exhibit A.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data: As set forth in Exhibit A.

Processing operations
The personal data transferred will be subject to the following basic processing activities: Processing to carry out the Services pursuant to the Agreement.

bugcrowd

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Service Provider will maintain technical, organizational, and physical safeguards to protect the security, confidentiality, integrity, and availability of Company Personal Data. Service Provider will not materially decrease the overall security of the Services during the Agreement.