bugcrowd

DATA PROCESSING ADDENDUM (v2.6)

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" with "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. **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 Module Two's obligations in the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**Standard Contractual Clauses**") as supplemented by Exhibit A attached hereto, the terms of which are incorporated herein by reference. 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.

e. **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 B 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.

f. **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 B.

g. **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.

h. **Bugcrowd Sub-Processors.** Customer agrees that Bugcrowd may engage sub-processors to Process Personal Data in accordance with the DPA. The list of Bugcrowd's sub-processors is available in Exhibit A. 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.

i. **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 Agreement 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 designed 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 C 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. 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:	**BUGCROWD INC.**
Signature:	Signature:
Print Name:	Print Name:
Print Title:	Print Title:

Exhibit A

Supplemental Terms for the Standard Contractual Clauses

This Exhibit A forms part of the DPA and supplements the Standard Contractual Clauses. Capitalized terms not defined in this Exhibit A have the meaning set forth in the DPA.

The parties agree that the following terms shall supplement the Standard Contractual Clauses:

1. **Supplemental Terms.** The parties agree that: (i) a new Clause 1(e) is added the Standard Contractual Clauses which shall read: "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."; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "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)."; (iii) the optional text in Clause 7 is deleted; (iv) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer must notify data exporter of any new subprocessors in accordance with Section 2.h of the DPA; (v) the optional text in Clause 11 is deleted; and (vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. **Annex I.** Annex I to the Standard Contractual Clauses shall read as follows:

   A. List of Parties

   Data Exporter: 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: The Services.
   Role: Controller.

   Data Importer: Bugcrowd Inc.
   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: The Services.
   Role: Processor.

   B. Description of the Transfer:

   Categories of data subjects whose personal data is transferred: As set forth in Exhibit B.

   Categories of personal data transferred: As set forth in Exhibit B.

   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: To the parties knowledge, no sensitive data is transferred.

   The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is transferred in accordance with the standard functionality of the Services, or as otherwise agreed upon by the parties.

   Nature of the processing: The Services.

   Purpose(s) of the data transfer and further processing: The Services.

   The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Data importer will retain personal data in accordance with the DPA.

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

Subprocessor	Type of Data Processed	Location
Datadog	Browser client IP, login activity, and accidental PII	New York, USA
Mailgun	Email Address	Texas, USA
Docusign	Tax Documents, NDA's etc	California, USA
Outreach	Email Address	Washington, USA
Drift	mixed	Massachusetts, USA
SFDC	Various Contact Details	California, USA
Clari	Email Address	California, USA
Marketo	Email Address	California, USA
Personyze	Email Address	Tel Aviv, Israel
Gotowebinar	Email Address	Massachusetts, USA
Highspot	Email Address sometimes	Washington, USA
Heap	IP and browsing history on-site	California, USA
Google Analytics	IP and browsing history on-site	California, USA
Tableau	Researchers#prime	Washington, USA
Gainsight	Email, activities on platform	California, USA
Google	email, document sharing, form response collection	California, USA
AWS	Broad processing activities	Washington, USA
Segment	Email, IP, and browsing history on-site	California, USA
Hellofax	Employee information over fax	California, USA

C. Competent Supervisory Authority: 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.

D. Clarifying Terms: The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Clauses will be provided upon data exporter's written request; (ii) the measures data importer is required to take under Clause 8.6(c) of the Clauses will only cover data importer's impacted systems; (iii) the audit described in Clause 8.9 of the Clauses shall be carried out in accordance with Section 7 of the DPA; (iv) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Clauses will be limited to the termination of the Clauses; (v) unless otherwise stated by data importer, data exporter will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Clauses; (vi) the information required under Clause 15.1(c) of the Clauses will be provided upon data exporter's written request; and (vii) notwithstanding anything to the contrary, data exporter will reimburse data importer for all costs and expenses incurred by data importer in connection with the performance of data importer's obligations under Clause 15.1(b) and Clause 15.2 of the Clauses without regard for any limitation of liability set forth in the Agreement.

3. **Annex II.** Annex II of the Standard Contractual Clauses shall read as follows:

Data importer shall implement and maintain 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.

4. **Annex III.** A new Annex III shall be added to the Standard Contractual Clauses and shall read as follows:

The UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**") is incorporated herein by reference.

Table 1: The start date in Table 1 is the effective date of the DPA. All other information required by Table 1 is set forth in Annex I, Section A of the Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to including the Appendix Information, effective as of the effective date of the DPA.

Table 3: The information required by Table 3 is set forth in Annex I and II to the Clauses.

Table 4: The parties agree that Importer may end the UK Addendum as set out in Section 19.

Exhibit B
Processing Details and Instructions

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

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

Data Importer: is Bugcrowd Inc., 300 California Street, Suite 220, San Francisco, CA 94104. Email for notices is privacy@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 in accordance with the DPA or as long as required under law, unless otherwise agreed to in writing.

Exhibit C
Security Measures

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

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