

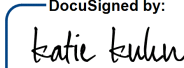
DATA PROCESSING ADDENDUM

BETWEEN CLIENT (CONTROLLER/EXPORTER)
Client Address Data Protection Key Contact:
AND BAZAARVOICE (DATA PROCESSOR/IMPORTER)
Bazaarvoice, Inc. 10901 Stonelake Blvd, Austin, TX 78759, USA Data Protection Key Contact: Christian Schmoll (Christian.schmoll@bazaarvoice.com)

This Data Processing Addendum ("DPA") shall be effective as of the date of the last signature ("DPA Effective Date") and shall be an integral part of the Principal Agreement concluded between the Client and Bazaarvoice.

STRUCTURE/LIST OF CONTENTS OF THIS DATA PROCESSING ADDENDUM
• Data Processing Addendum (DPA) • Schedule 1: Details of Processing • Schedule 2: Technical and Organisational Measures • Schedule 3: Sub-Processors • Schedule 4: UK Addendum

Client
Name and title/function
Date:
Signature:

Bazaarvoice
Name and title/function
Katie Kuhn Sr. Director, Finance
Date:
12/2/2022
Signature:
DocuSigned by:  4D40205316B7488...



DEFINITIONS

"Appropriate safeguards" means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time.

"Client Personal Data" means the personal data processed by Bazaarvoice on behalf and on instruction of the Client in connection with the provision of the services provided by Bazaarvoice;

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Data Protection Laws, the controller or the specific criteria for its nomination may be provided for by Data Protection Laws.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"Data Subject" means an identified or identifiable natural person whose rights are protected by Data Protection Laws.

"Data Protection Laws" means any and all laws as defined herein, codes and regulations as applicable to, the Services from time to time limited to: (i) General Data Protection Regulation (EU) 2016/679 ("GDPR"); (ii) Privacy and Electronic Communication (EC Directive) Regulations 2003 and other similar regulations as applicable in France; (iii) the UK General Data Protection Regulation (UK GDPR) (iv) the Swiss Federal Act on Data Protection (v) California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations ("CCPA"); (vi) the California Privacy Rights Act; (vii) the Virginia Consumer Data Protection Act; (viii) the Colorado Privacy Act and (ix) Privacy Act 1988 of Australia.

"EEA" means the European Economic Area.

"GDPR" means Regulation (EU) 2016/679 (the "EU GDPR") or, where applicable the "UK GDPR" as defined in the UK Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019.

"Personal Data" means any information relating to an identified or identifiable natural person and subject to Data Protection laws which is submitted by or collected and processed on behalf and on instruction of Client.

"Personal Data Breach" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Personal Data.

"Process/Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Services" has the meaning given to the term under the Principal Agreement.

"Standard Contractual Clauses" means Module Two (controller to processor) and/or Module Three (processor to processor) annexed to Commission Implementing Decision (EU) 2021/914.

"Sub-Processor" shall include: (i) an entity engaged by the Data Processor in order to perform Processing of Personal Data related to this Agreement; and (ii) entities defined as a "Sub-processor" under the Applicable Data Protection Law;

"Supervisory Authority" means any local, national, or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other legislative body responsible for administering Data Protection Laws.

1. SUBJECT OF THE DPA AND ROLE OF THE PARTIES

- 1.1 Bazaarvoice and Client entered into one or more written services principal Agreement (the "Principal Agreement(s)") which involve Processing of Personal Data of Data Subjects subject to Data Protection Laws in the context of the Services. All capitalized terms not defined herein shall have the meaning set forth in the Principal Agreement.
- 1.2 Pursuant to the Principal Agreement, Bazaarvoice provides services to Client which may include hosted online customer feedback services, and associated consulting and support. This DPA specifies the obligations of the Parties regarding data protection, and applies to all activities related to the Principal Agreement in which Bazaarvoice processes Personal Data on behalf of and in accordance with the instructions of the Client as its data processor. The scope of this DPA shall also govern Personal Data of third parties as a sub-processor of the Client.
- 1.3 Unless specifically agreed in writing by the parties, the parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Data Controller, Bazaarvoice is a Data Processor and that any subcontractors engaged by Bazaarvoice pursuant to the requirements set forth herein will be Sub-Processor.



- 1.4 The parties agree to comply with the provisions of this DPA with respect to the processing of any and all Personal Data collected on behalf of or submitted by the Client in relation to the provision or receipt of the Services. In accordance with Data Protection Laws, the parties enter into this DPA which shall govern the Processing of Personal Data of Data Subjects subject to Data Protection Laws in the context of the Services. This DPA, is incorporated into the Principal Agreement by reference and as an annex, is an integral part of the Principal Agreement.
- 1.5 The Services are provided by Bazaarvoice under a Software as a Service (SaaS) model. Namely, Client brings its own data, largely controls the upload and handles directly the use of Personal Data that is Processed in conjunction with the Services. It is therefore the sole responsibility and liability of Client to ensure that Personal Data is collected and transmitted to Bazaarvoice in compliance with applicable Data Protection Laws and, in particular, to have a legal basis for Processing and to properly inform Data Subjects of the collection and Processing of their Personal Data.

2. DATA PROCESSING

The Processing of Personal Data by Bazaarvoice for Client is such as is strictly required in the performance of the contracted Services under the Principal Agreement. Further details of the Personal Data and Data Subjects required to provide the contracted Services can be found in **Schedule 1**.

3. OBLIGATIONS OF THE PROCESSOR

- 3.1 Bazaarvoice shall in relation to Personal Data processed by Bazaarvoice on behalf of Client as a Data Processor:
 - (a) process the Personal Data only on the instructions of the Client, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by law to which Bazaarvoice is subject. In such a case, Bazaarvoice shall inform Client of that legal requirement before Processing, unless that law prohibits such information on grounds of public interest. Client's instructions may be specific instructions or standing instructions of general application in relation to the performance of Bazaarvoice's obligations under the Principal Agreement; and
 - (b) ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and
 - (c) take all measures required pursuant to Article 32 of the GDPR and clause 10 of this DPA with respect to the security of Processing; and
 - (d) respect the conditions of the Data Protection Laws and clause 7 of this DPA for engaging a Sub-Processor; and
 - (e) assist Client in ensuring compliance with the obligations under Data Protection Laws with respect to:
 - (i) security of Processing; and
 - (ii) notifications to the Supervisory Authority in case of any Personal Data Breach; and
 - (iii) communications to Data Subjects by the Client in response to any Personal Data Breach; and
 - (iv) as in accordance with Article 28(3) of the GDPR, Bazaarvoice will cooperate and assist Client with any data protection impact assessments which are referred to in Article 35 of the GDPR or with any regulatory consultations that Client is legally required to make in respect of Personal Data, taking into account the nature of the Processing and the information made available to Bazaarvoice;
 - (v) prior consultation with a Supervisory Authority regarding high risk Processing;
 - (f) at Client's choice, delete or return all the Personal Data to Client:
 - (vi) once Processing by Bazaarvoice of any Personal Data is no longer required for the purpose of Bazaarvoice's performance of its relevant obligations under this DPA or the Principal Agreement(s) due to termination for any reason; or
 - (vii) on request by the Client;

and delete existing copies unless Data Protection Laws requires storage of the Personal Data and inform the Client of such requirement;
 - (g) subject to clause 7, make available to Client all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits. For this purpose, Bazaarvoice may provide certifications, reports or report extracts from independent entities (e.g. auditors, inspectors, data security officers, IT security departments, data protection auditors, quality assurance auditors) or appropriate certification from an IT security or data security audit.
- 3.2 **Notification of access requests and complaints:** To the extent legally permitted, Bazaarvoice shall promptly notify Client of:
 - (i) any request received directly by Bazaarvoice from a Data Subject to exercise the Data Subject's right of access or have



copies of Personal Data, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making pertaining to his or her Personal Data; or (ii) any complaint or allegation made to Bazaarvoice relating to Personal Data, either from a Data Subject, a Supervisory Authority or other third party (each a "Data Protection Communication"). In addition and in accordance with Data Protection Laws, Bazaarvoice shall:

- 3.2.1 not respond to a Data Protection Communication unless Bazaarvoice is authorized to do so by Client or Bazaarvoice is legally compelled to respond;
- 3.2.2 When taking into account the nature of the Processing, Bazaarvoice shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Protection Communication under Data Protection Laws;
- 3.2.3 In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Protection Communication, Bazaarvoice shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Protection Communication, to the extent Bazaarvoice is legally permitted to do so and the response to the Data Protection Communication is required under Data Protection Laws. To the extent legally permitted, Client shall be responsible for any costs arising from Bazaarvoice's provision of such assistance.
- 3.3 Bazaarvoice shall immediately notify Client if, in its opinion, an instruction infringes Data Protection Laws, provided that to the maximum extent permitted by mandatory law, Bazaarvoice shall have no liability arising for any losses, costs, expenses or liabilities arising from or in connection with any Processing in accordance with the Client's Processing instructions, following the Client's receipt of that notification.
- 3.4 Bazaarvoice shall not unreasonably withhold, delay or condition its agreement to any change to this DPA requested by Client in order to ensure Client can comply with Data Protection Laws.

4. TECHNICAL/ORGANISATIONAL MEASURES

- 4.1 In relation to the Processing of Personal Data, Bazaarvoice shall implement and maintain, at its cost and expense, a suitable information security program taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of Processing the Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of the Clients Users. Such program shall include technical and organisational measures no less stringent than those set out in **Schedule 2**.
- 4.2 Technical and organisational measures are subject to technical advancements and future developments. Bazaarvoice is, therefore, permitted to make use of adequate alternate measures in this respect. Such alternate measures may not, however, fall below the level of security stipulated in the Data Protection Laws for these measures. Substantive changes shall be properly documented and notified to Client.

5. SUB-PROCESSORS

- 5.1 The provision of the Services by Bazaarvoice requires the use of Subprocessors. Client hereby authorizes Bazaarvoice to use the sub-processors listed under **Schedule 3**.
- 5.2 Bazaarvoice shall expressly notify the Client in writing at least 14 days in advance of any intended changes concerning the inclusion or replacement of Subprocessors and the Client shall be given the opportunity to object to such changes for material reasons.
- 5.3 Bazaarvoice shall impose obligations on all Subprocessors by way of a contract or other legally binding agreement that provide at least substantially the same level of protection for the Personal Data Processed under this DPA as the obligations provided for in this DPA, in particular by providing safeguards for the implementation of appropriate technical and organizational measures so that the Processing complies with the requirements of (i) this DPA and (ii) the Data Protection Laws. If the Subprocessor fails to comply with its data protection obligations, Bazaarvoice shall remain fully liable to the Client for the performance of the Subprocessor's obligations.
- 5.4 If the Client is located in the EEA or Switzerland and Bazaarvoice uses a Subprocessor in a third country where an adequate level data protection is not ensured, Bazaarvoice will provide Appropriate Safeguards in relation to the Subprocessor.
- 5.5 Services that Bazaarvoice uses from third parties as a purely ancillary service in order to carry out its business activities are not considered subcontracting relationships. This includes, for example, cleaning services, pure telecommunication services without concrete reference to services that Bazaarvoice provides for the Client, postal and courier services, transport services, guarding services. Bazaarvoice is nevertheless obliged, also in case of ancillary services provided by third parties, to ensure that adequate precautions and technical and organizational measures have been taken to ensure the protection of personal data. The maintenance and servicing of IT systems or applications shall constitute subprocessing under this DPA and a subcontracting relationship requiring consent if the maintenance and servicing concern such IT systems that are also used in



connection with the provision of services for the Client and personal data processed on behalf of the Client can be accessed during the maintenance.

6. INTERNATIONAL DATA TRANSFERS

6.1 The provision of the Services under the Principal Agreement may require the transfer or processing of the Personal Data processed under the Service Order. For the purposes of GDPR, this will mean that data is transferred to third countries outside the EEA, including but not limited to the United Kingdom and Switzerland.

6.2 The Parties agree that the terms of the Standard Contractual Clauses Module Two (Controller to Processor) and Module Three (Processor to Processor) apply to any transfers of Customer Personal Data falling within the scope of the GDPR from Customer (as data exporter) to Bazaarvoice (as data importer) as specified below:

(a) Module Two shall apply in instances where Customer functions as a controller, whereas Bazaarvoice functions as a processor. Module Three shall apply in the case where Customer functions as a processor on behalf of Customer's customers where Customer and Customer's customer have concluded a data processing agreement in relation to the processing of personal data of Customer's customers.

(b) To the extent that the processing of Customer Personal Data is subject to UK data protection laws, the UK Addendum set out in **Schedule 4** shall apply.

6.3 The Standard Contractual Clauses shall apply as follows:

- (a) Annex I.A (List of Parties) shall be deemed to be Client, Client Affiliate, and Bazaarvoice;
- (b) Annex I.B (Description of Transfer) shall be deemed to incorporate the information in Schedule 1;
- (c) Annex I.C (Competent Supervisory Authority) shall be deemed to refer to the supervisory authority of Bavaria, Germany (BayLDA) in the EEA and the ICO in the UK;
- (d) Annex II (Technical and Organisational Measures) shall be deemed to incorporate the information in Schedule 2;
- (e) in Clause 7, the optional docking clause shall apply;
- (f) or the purposes of Clause 8.1 (a), the Principal Agreement and this DPA shall be the Client's final instructions for the processing of Client Personal Data;
- (g) for the purposes of Clause 9 of the Standard Contractual Clauses, the Client gives Bazaarvoice the general authorisation to engage sub-processors from an agreed list and **Schedule 3** sets out the list of sub-processors agreed by the Parties and the time period for information in advance of any intended changes to the list through the addition or replacement of sub-processors shall be at least 14 days.
- (h) in Clause 11, the optional language shall not apply;
- (i) the certification of deletion described in Clause 16 (d) shall be provided by Bazaarvoice to Client upon Client's written request;
- (j) for the purposes of Clause 15 (1) (a), Bazaarvoice shall notify Client and not the relevant data subject(s) in case of government access requests, and Client shall be solely responsible for notifying the relevant data subjects as necessary;
- (k) in Clause 17, option 1 shall apply and the Standard Contractual Clauses shall be governed by German law; and
- (l) in Clause 18 (b), disputes shall be resolved before the courts of Munich, Germany;

6.4 In the event of any conflict between the applicable Standard Contractual Clauses and the main body of this DPA, the provisions of the applicable Standard Contractual Clauses shall prevail. Any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

7. AUDIT

7.1 Bazaarvoice uses external auditors to validate the adequacy of its security standards and controls (Bazaarvoice Audit). Bazaarvoice Audit activities: (i) will be performed by Bazaarvoice no more than once per annum; (ii) will be performed by independent third-party security professionals at Bazaarvoice's selection and expense; and (iii) will result in the generation of an audit report (Audit Report), which will be deemed Bazaarvoice's confidential information.

7.2 At Client's written request, Bazaarvoice will provide Client with the Audit Report summarizing the elements set forth in Section 7.1 above so that Client can reasonably verify Bazaarvoice's compliance with its obligations under this DPA.

7.3 In accordance with Clause 3.1 (g) and to the extent required by Data Protection Laws, including where mandated by Client's Supervisory Authority, the Client or Client's Supervisory Authority may perform an audit (collectively, "Client Audit") subject



to Bazaarvoice will contribute to such Client Audits by providing Client or Client's Supervisory Authority with the information and assistance reasonably necessary to conduct the Client Audit, including any relevant records of Processing activities applicable to the Services. Provided always that the Client:

- (a) notifies Bazaarvoice in writing with reasonable notice (not less than 30 working days) that such request for information, audit and/or inspection is required by Client;
- (b) that where a third party is engaged to conduct an audit that said third party signs a Bazaarvoice NDA;
- (c) that parties mutually agree the scope of any such Client Audit;
- (d) ensures that all information received or generated by the Client or its auditor(s) in connection with the requests for information, inspections and audits is kept strictly confidential (except for disclosure to the Supervisory Authority or as otherwise required under the Data Protection Laws) and;
- (e) ensures that the audit or inspection takes place during normal business hours and causes as little disruption as possible to the business operations of Bazaarvoice, the business operations of the Sub-processors and the business operations of any other clients of Bazaarvoice, and provided that no more than one such audit or inspection shall be conducted in any 12-month period, unless required by a competent regulatory authority.

For the avoidance of doubt any external penetration testing of any of Bazaarvoice's systems is strictly prohibited.

- 7.4 If a third party is to conduct the Client Audit, the third party must be approved by Bazaarvoice (except if such third party is a competent Supervisory Authority). Bazaarvoice will not unreasonably withhold its consent to a third-party auditor requested by Client. The third party must execute a written confidentiality agreement acceptable to Bazaarvoice or otherwise be bound by a statutory confidentiality obligation before conducting the Client Audit.
- 7.5 Client will provide Bazaarvoice any audit reports generated in connection with any Client Audit, unless prohibited by Applicable Law or otherwise instructed by a Supervisory Authority. Client may use the audit reports only for the purposes of meeting Client's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are Confidential Information of Bazaarvoice under the terms of the Principal Agreement.
- 7.6 Any Client Audits are at Client's sole expense. The parties will negotiate in good faith with respect to any charges or fees that may be incurred by Bazaarvoice to provide assistance with a Client Audit that requires the use of resources different from or in addition to those required for the provision of the Services.

8. REPORTING VIOLATIONS

- 8.1 Bazaarvoice shall in all cases notify the Client, without undue delay and where feasible not later than 48 hours after becoming aware, of any Personal Data Breach or any breach of the specifications set down in the Principal Agreement, and provide the Client with details of any Personal Data Breach. Such notification shall at least:
 - (a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
 - (c) describe the measures taken or proposed to be taken by the processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

- 8.2 It is recognized that, pursuant to Data Protection Laws, an obligation to provide information may exist in the event that Personal Data is lost or unlawfully accessed/disclosed. Therefore, the Client should be notified of such incidents, regardless of the cause. This also applies to serious disruptions in operations or other irregularities in handling the Client's Personal Data. In cooperation with the Client, Bazaarvoice shall take appropriate steps to secure the data and mitigate possible negative effects on the affected parties.

9. DELETING DATA

- 9.1 Should the Client issue a deletion instruction in writing to Bazaarvoice, the latter is thereby authorized and obligated to commence the permanent deletion no later than one week after receipt of such instruction unless Data Protection Laws require storage of the Personal Data.
- 9.2 Bazaarvoice will commence permanent deletion of the Client's Personal Data upon expiry or termination of the Principal Agreement.



- 9.3 Documentation which serves to provide proof that data Processing occurred properly and pursuant to contract shall be retained by Bazaarvoice beyond the term of the Principal Agreement in accordance with the appropriate retention schedules.
- 9.4 For the avoidance of doubt, Client acknowledges and agrees that as in accordance with Art. 6 (1) lit. f) GDPR Bazaarvoice retains the right to retain key elements of the Personal Data ("Key Data") collected and processed in connection with Services for the purposes of anti-fraud monitoring as laid out under the Authenticity Policy which can be found at the page: www.bazaarvoice.com/legal/authenticity-policy.
- 9.5 For the purposes of the Agreement and this Section 9, "Key Data" means any personal data including but not limited to "Author IP address" and "Author Device Fingerprint" that is required strictly for the purposes of anti-fraud and authenticity services that are a mandatory requirement of the Bazaarvoice Services.

10. UNITED STATES PRIVACY LAWS

- 10.1 Client discloses Personal Data to Bazaarvoice for a business purpose.
- 10.2 Bazaarvoice is prohibited from: (i) selling Client's Personal Data; (ii) retaining, using, or disclosing Client's Personal Data for any purpose other than for the specific purpose of performing the Services specified in the Principal Agreement; (iii) retaining, using, or disclosing Client's Personal Data outside of the Principal Agreement or direct business relationship between Client and Bazaarvoice and (iv) combining or updating Personal Information it receives from or on behalf of Client with Personal Information that it received from another source except as permitted by Data Protection Laws or as directed by Client.
- 10.3 Certification. By signing this DPA, Bazaarvoice hereby certifies that in receiving Client's Personal Data, Bazaarvoice understands the requirements and restrictions associated with its status as a Service Provider, and shall comply with the applicable requirements set forth in the Data Protection Laws in effect in the United States and any implementing regulations.
- 10.4 For the purpose of this Section 6, the terms "consumer", "commercial purpose" and "sale" shall have the meaning given to them by the CCPA.

11. LIABILITY

The liability of each party under this DPA shall be subject to the exclusions and limitations of liability set out in the Principal Agreement. Any reference to "limitation of liability" of a party in the Principal Agreement shall be read to mean the aggregate liability of a party and all of its Affiliates under the Principal Agreement and this DPA.

12. GENERAL PROVISIONS

- 12.1 The Processing of Personal Data under this DPA is governed by the law of the Principal Agreement and supersedes and replaces any prior agreements in respect of the processing of personal data. Any disputes between the parties relating to the Processing of Personal Data under this DPA will be subject to the exclusive jurisdiction of the courts set forth in the Principal Agreement.
- 12.2 With respect to the subject matter described above, this DPA, including the Annexes attached hereto, constitutes the entire agreement between the parties and supersedes all prior communications, representations, understandings, and agreements, whether oral, electronic or written.
- 12.3 To the extent of inconsistencies between the provisions of this DPA and other agreements between the parties, including but not limited to the Principal Agreement, the provisions of this DPA shall prevail. In cases of doubt, this DPA shall prevail, in particular, where it cannot be clearly established whether a clause relates to a party's data protection obligations.
- 12.4 This DPA may only be modified by a written amendment signed by authorized representatives of each of the parties.
- 12.5 This DPA will become effective as of the date the parties have executed it and, notwithstanding expiry of the term of the Principal Agreement, will remain in effect until, and will automatically expire upon, deletion of all Personal Data by Bazaarvoice and/or any applicable Subprocessors.
- 12.6 Unless stated otherwise, each party shall perform its obligations under this DPA at its own cost.
- 12.7 If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

SCHEDULE 1: DETAILS OF PROCESSING

Categories of data subjects whose personal data is processed/transferred:

Client's customers and users of Client's products and services and visitors of Client's websites

Categories of personal data transferred:

user email address, user IP address, user device fingerprint, timestamp, user-generated content

Sensitive data transferred:

None (unless any sensitive data is contained in the user-generated content)

Frequency of the transfer:

continuously during the term of the contract

Nature of the processing:

Provision of a software platform (software as a service) that enables Client to collect, display, and distribute user-generated content, as defined in further detail in the Principal Agreement and the respective Service Orders

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

Fulfilment of a contract for the use of the Bazaarvoice software platform

Duration for which the personal data will be stored or, if this is not possible, the criteria for determining this duration:

Duration of the contract

In the case of data transfers to (sub)processors, the subject, type and duration of the processing shall also be indicated:

*For transfers to sub-processors, specify subject matter, nature and duration of the processing: as set out in **Schedule 3**.*

Competent supervisory authority:

The data protection supervisory authority of Bavaria, Germany (Bayerische Landesamt für Datenschutzaufsicht).

SCHEDULE 2: TECHNICAL AND ORGANISATIONAL MEASURES

Minimum technical and organisational measures implemented by Bazaarvoice for the security and protection of Personal Data:

- 1. Measures for the Prevention of Unauthorised Access to Commercial Premises and Installations Used for Processing Personal Data**
 - Physical access to corporate sites is controlled via badge access, which are to be present with the employee at all times. All employees and contractors requiring physical access to a site receive this access during the New Hire Onboarding process controlled by People Operations, and upon separation from the company, a termination process also owned by People Operations revokes badge/key authority.
 - Vendors, contractors, and other visitors requiring temporary access to a site are required to register at the front desk where a badge is issued allowing access to only main office areas and they are controlled and monitored. Visitors have to register at the front desk, are issued a temporary visitor identification tag, and are to be always escorted.
 - Physical access to critical IT areas is restricted to those with a legitimate business need. Systems and data processing is hosted in a vetted and top industry cloud hosting provider.
- 2. Measures for the Prevention of Unauthorised Access to IT Systems**
 - Unique accounts and logons are required for users' daily activity.
 - Passwords are to be at least 8 characters long and comply with at least three of the four complexity requirements.
 - Two-factor authentication is required for user login to the network.
 - Access to IT systems (network equipment, devices, servers, and applications) is controlled by the Bazaarvoice Information Security Policy
 - Remote access to Bazaarvoice corporate infrastructure is controlled via Virtual Private Network, using two-factor authentication. Access to VPN is granted for Bazaarvoice employees, is controlled via Active Directory and managed by People Operations New Hire/Termination processes.
 - Bazaarvoice wireless network is secured according to industry standards and leverages a minimum of 128 bit key. Two wireless networks are provided, one for guest access with a published password on the intranet, and one for employees with access to corporate network where access is pre-configured by IT personnel on authorized equipment.
- 3. Data Access Controls Measures**
 - Authorised users only have access to data which are in their area of responsibility and, where Processing Personal Data, that these data cannot be read, copied, changed or deleted without appropriate authorisation.
 - Employees working in the operational area only are authorised to access the database and administer it, and also to modify and delete data. The logins and all database accesses of all employees working in the operational area are logged.
 - The implementation engineer assigned to the client has access to the client data and can view and process these, but only using tools from Bazaarvoice and not via the interface of the database management system. All changes to the data made using these tools are logged.
- 4. Disclosure Control Measures**
 - The data in the Bazaarvoice databases are protected during transfer between the Data Controller and Bazaarvoice using TLS encryption.
 - The token assigned uniquely to a user and used to identify the user is encoded before transfer to Bazaarvoice using a unique, client-specific token which is supplied to the client as a key.
- 5. Input Control Measures**
 - The administration tasks performed on servers are logged by the Operations Department, including the bash and login history.



- Data manipulations including addition, deletion, approval or rejection of content data are logged using Bazaarvoice's content moderation system.
- Logging of data changes is also performed via the Bazaarvoice Workbench portal tool.

6. Job Control Measures

Measures to ensure that personal data are only processed on behalf of the Controller on the express instruction of the Controller:

- Background checks are performed on all new employees, as permitted by local laws.
- There are mandatory training courses, including data protection and information security for new employees.
- New employees have only limited access rights until the training measures have been completed during the first week of employment.
- Secure coding training is required for all personnel who develop code.
- All development work is inspected in accordance with the peer review Principal, ensuring that all system changes are reviewed in advance by two people.
- A violation of the company's protocols and procedures, results in immediate sanctions up to and including the withdrawal of all access rights and, where appropriate, termination.

7. Availability Control Measures:

- Bazaarvoice maintains a Business Continuity Program which applies to processes critical to Bazaarvoice operations.
- Appropriate availability controls and processes are in place to ensure availability of operations in the cloud hosting environment.
- Virus protection is required on all desktop and laptop computers in the Bazaarvoice network.
- The server environment is predominantly linux-based; additional controls are in place, such as web application firewalls, system hardening, patch management and reduced access controls to protect the production environment.
- All source code, build, and configuration elements are managed in a source code repository

8. Security Testing and Evaluation Measures:

- Internal and external vulnerability scans are performed no less than quarterly by the Bazaarvoice Security team. The results are documented, reviewed by the Information Security Officer (ISO) and prioritised by the cross-organisational Security Leadership Team. Critical and high findings are closed within 30 days pending environmental impact, and informational findings are acted upon on a case by case basis in line with Risk Management processes.
- An external penetration test is performed annually by a third party. The results are documented, reviewed by the ISO and prioritized by the cross-organisation Security leadership team. Findings and remediation plans are documented and resolved within timelines per severity.

9. Separation Control Measures:

- Client data is logically separated and stored using a unique customer ID. A client will under no circumstances be able to access data of other clients.
- Due to the nature of their role, employees of the operations department have access to client data in order to troubleshoot and support client needs as they arise.
- Implementation engineers only have access to the data related to projects for which they are responsible, and only via tools supplied by Bazaarvoice.



SCHEDULE 3: SUB-PROCESSORS

The controller has authorised the use of the sub-processors listed at:

https://knowledge.bazaarvoice.com/wp-content/knowledge/en_US/vendorlist.html

SCHEDULE 4: UK ADDENDUM

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

This 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 start date of this Data Transfer Addendum shall be the DPA Effective Date.
Parties' Details	The Exporter and Importer details shall be the Client and Bazaarvoice, as specified above.
Key Contact	The Exporter and Importer key contacts shall be as defined above (on top of the DPA)

Table 2: Selected SCCs, Modules and Selected Clause

Addendum EU SCCs	
-------------------------	--

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 Addendum is set out in:

Annex 1A: List of Parties	Listed above
Annex 1B: Description of Transfer	See Schedule 1 above
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data	See Schedule 2 above
Annex III: List of Sub processors	See Schedule 3 above

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Neither Party may end this Addendum as set out in Section 19.
---	---

Part 2: Mandatory Clauses

Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- 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 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 Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

- Where this 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	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this 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 Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 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 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 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 Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this 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 Addendum, UK Data Protection Laws applies.
7. If the meaning of this 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 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 Addendum and the Addendum EU SCCs (as applicable), the Approved 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 Addendum.
11. Where this 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 Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This 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 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 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 Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this 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 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 Addendum which:
 - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
 - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
 - a. its direct costs of performing its obligations under the Addendum; and/or



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