COVER PAGE

Attached please find UserVoice's Data Processing Addendum ("DPA") addressing the parties' obligations and rights in relation to the processing of personal data. This DPA forms part of the Services Agreement or other written agreement between you and UserVoice. To complete this DPA, we request that you complete the information in the signature box, sign on Page 4, and submit the completed and signed DPA to support@uservoice.com.

If you have questions about this DPA, please contact your UserVoice contact or email support@uservoice.com.

USERVOICE'S DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into between UserVoice, Inc. ("UserVoice") and Customer (jointly "the Parties"), and forms a part of the Services Agreement between the Parties, and reflects the Parties' agreement with regard to the Processing of Personal Data in accordance with the requirements of the Data Protection Laws.

By signing the DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent UserVoice Processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

This DPA is effective on the date that it has been duly executed by both Parties ("Effective Date"), and amends, supersedes and replaces any prior data processing agreements that the Parties may have been entered into. Any modifications to the terms of this DPA (whether handwritten or otherwise) will render this DPA ineffective unless UserVoice has separately agreed to those modifications in writing.

1. DEFINITIONS

1.1. "Authorized Affiliate" means Customer's Affiliate(s) which (a) are subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom; (b) are permitted to use the Services pursuant to the Agreement between Customer and UserVoice; and (c) have not signed their own Services Agreement with UserVoice and are not "Customers" as defined under this DPA.

1.2. "Affiliate" means any entity that directly or indirectly controls, is controlled by or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.3. "Covered Services" or "Services" means the services that are ordered by the Customer from UserVoice involving the Processing of Personal Data on behalf of the Customer.

1.4. "Customer" means the entity that signed the Services Agreement and that determines the purposes and means of Processing of Personal Data. The Customer is considered the "Controller" of the Personal Data provided pursuant to this DPA.

1.5. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored or otherwise Processed.

1.6. "Data Protection Laws" means any applicable law, statute, law, regulation or order by governmental authority of competent jurisdiction, or any judgment, decision, decree, injunction, writ, order, subpoena, or like action of any court, arbitrator or other government entity, and at all times during the term of the Service Agreement, including the laws of the European Union ("EU") Data Protection Act 1998, the EU General Data Protection Regulation ("GDPR"), as amended or replaced from time to time, and any other foreign or domestic laws to the extent that they are applicable to a party in the course of its performance of the Contract.

1.7. "Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'), which information is subject to the GDPR or the laws of non-EU EEA countries that have formally adopted the GDPR, which is provided by or on behalf of Customer and Processed by or on behalf of UserVoice pursuant to the Services Agreement.

1.8. "Regulator" means any supervisory authority with authority under Data Protection Laws over all or any part of the provision or receipt of the Services or the Processing of Personal Data.

1.9. "Services Agreement" means any agreement between UserVoice and Customer under which Covered Services are provided by UserVoice to Customer.

1.10. "Subprocessor" means any Processor engaged by UserVoice to Process Personal Data on behalf of UserVoice.

1.11. Terms such as "Data Subject", "Processing", "Controller", "Processor" and "Supervisory Authority" shall have the meaning ascribed to them in the Data Protection Laws.

2. SERVICES AGREEMENT

2.1. This DPA supplements the Services Agreement and in the event of any conflict between the terms of this DPA and the terms of the Services Agreement, the terms of this DPA prevail with regard to the specific subject matter of this DPA.

2.2. Any provisions contained in this DPA that would not apply to the Parties but for the GDPR shall not apply to the Parties until May 25, 2018 and thereafter.

3. **DATA PROTECTION LAWS**

3.1. **Roles of the Parties.** The Parties acknowledge and agree that UserVoice will Process the Personal Data in the capacity of a Processor and that Customer will be the Controller of the Personal Data.

3.2. **DPO**. Upon enforcement of the GDPR, the Parties, to the extent required by the GDPR, will each designate a data protection officer (a "DPO") and provide their contact details to the other Party where required by the Data Protection Laws.

4. **OBLIGATIONS OF THE CONTROLLER**

4.1. **Instructions**. Customer warrants that the instructions it provides to UserVoice pursuant to this DPA will comply with Data Protection Laws.

4.2. **Data Subject and Regulator Requests**. Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under Data Protection Laws and all communications from Regulators that relate to the Personal Data, in accordance with Data Protection Laws. To the extent such requests or communications require UserVoice's assistance, Customer shall immediately notify UserVoice in writing of the Data Subject's or Regulator's request.

4.3. **Notice, Consent and Other Authorizations**. Customer agrees that the Personal Data will be collected in compliance with Data Protection Laws, including all legally required consents, approvals and authorizations. Upon UserVoice's request, Customer shall provide adequate proof of having properly obtained all such necessary consents, authorizations and required permissions.

5. **DETAILS OF PROCESSING ACTIVITIES**

5.1. The following table sets out the details of Processing:

Purposes for which the Personal Data shall be processed	UserVoice will Process Personal Data for the purpose of providing the Covered Services described in the Services Agreement.
Description of the categories of the data subjects	Personal information is processed about UserVoice's Customers and their employees and end-users where necessary to provide the Covered Services.
Description of the categories of Personal Data	Personal data processed includes: name, email address, ip address, billing address, and company name or affiliation.

6. **OBLIGATIONS OF THE PROCESSOR**

6.1. **Scope of Processing**. UserVoice will Process the Personal Data on documented instructions from Customer in such manner as is necessary for the provision of Services under the Service Agreement, except as may be required to comply with any legal obligation to which UserVoice is subject. UserVoice shall inform Customer if, in its opinion, the execution of an instruction relating to the Processing of Personal Data could infringe on any Data Protection Laws. In the event UserVoice must Process or cease Processing Personal Data for the purpose of complying with a legal obligation, UserVoice will inform the Customer of that legal requirement before Processing or ceasing to Process, unless prohibited by the law.

6.2. **Data Subject and Regulator Requests**. UserVoice will promptly notify Customer in writing of any complaints, questions or requests received from Data Subjects or Regulators regarding the Personal Data. Taking into account the nature of the Processing and to the extent reasonably possible, UserVoice will assist Customer in fulfilling Customer's obligations in relation to Data Subject requests under applicable Data Protection Laws.

6.3. **Retention**. Upon Customer's written request, and at Customer's expense, UserVoice will destroy all Personal Data in its possession or return the Personal Data to Customer, as requested. Notwithstanding the foregoing, (i) any return or destruction shall be subject to all applicable laws, regulations and UserVoice compliance policies, and (ii) nothing in this DPA shall be deemed to require the alteration, modification, deletion or destruction of backup tapes or other backup or archived media made in the ordinary course of business.

6.4. **Disclosure to Third Parties.** Except as expressly provided in this DPA, UserVoice will not disclose Personal Data to any third party without Customer's consent. If requested or required by a competent governmental authority to disclose the Personal Data, to the extent legally permissible and practicable, UserVoice will provide Customer with sufficient prior written notice in order to permit Customer the opportunity to oppose any such disclosure.

6.5. **Confidentiality**. UserVoice will restrict access to the Personal Data to its personnel (and the personnel of its Affiliates) and to its Subprocessors who need access to meet UserVoice's obligations under the Services Agreement. Further, UserVoice will ensure that all such personnel and Subprocessors are informed of the confidential nature of the Personal Data and have undertaken training on how to handle such data. UserVoice will ensure that personnel authorized to Process the Personal Data are subject to binding confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

6.6. **GDPR Articles 32-36**. Upon enforcement of the GDPR, and taking into account the nature of the Processing and the information available to UserVoice, UserVoice will provide reasonable assistance to Customerin complying with its obligations under GDPR Articles 32-36, which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation.

6.7. **Information Security**. Taking into account the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, UserVoice agrees to implement and maintain adequate organizational and technical measures to protect the confidentiality, integrity and availability of the Personal Data it Process on Customer's behalf, including, at a minimum:

Physical Access Control: housing databases on servers located in secure, off-site facilities that maintain a biometric security system to track facility access and digital security video surveillance.

System Access Control: implementing unique logins and passwords for all users with system access, server firewalls, current malware, antivirus and security software.

Data Access Control: limiting access to those personnel who require such access to perform the Services Agreement, offering training for personnel on access rights and maintaining policies for the control and retention of back-up copies.

Transmission Control: encrypting Personal Data transferred between a user's web browser and UserVoice's software and encrypt backups.

Input Control: implementing unique logins to monitor activities.

Job Control: using or disclosing Personal Data solely for the purpose of performing, and only to the extent needed to perform UserVoice's obligations under the Services Agreement.

Availability Control: maintaining encrypted backup hosted in a second separate facility and engaging multiple suppliers for network connectivity and redundant power supplies including on-site power generation in the event of emergency.

Separation Control: implementing logical data separation determined by role-based permission.

7. AUDIT

7.1. **Scope**. UserVoice will maintain records of its Processing activities as required by the Data Protection Laws and will make available to Customer information reasonably necessary to demonstrate its compliance with the obligations set out in this DPA. Customer's inspection rights under this DPA do not extend to UserVoice's employee payroll, personnel records or any portions of its sites, books, documents, records, or other information that do not relate to the Services or to the extent they pertain to third parties.

7.2. **Process**. Subject to reasonable written notice from Customer, UserVoice will permit audits conducted by a third-party auditor acting on Customer's behalf to enable Customer to verify that UserVoice is in compliance with the obligations under this DPA. Audits and inspections will be carried out at mutually agreed times during regular business hours.

7.3. **Confidentiality.** All information obtained during any such request for information or audit will be considered UserVoice's confidential information under the Services Agreement and this DPA. The results of the inspection and all information reviewed during such inspection will be deemed UserVoice's confidential information. The third party auditor may only disclose to Customer specific violations of this DPA if any, and the basis for such findings, and shall not disclose any of the records or information reviewed during the inspection.

8. CONTRACTING WITH SUBPROCESSORS

Customer hereby consents to UserVoice's engagement of Subprocessors in connection with the processing of the Personal Data. Upon written request, UserVoice will make the list of applicable Subprocessors available to Customer. Customer may reasonably object to any new Subprocessor, in which case UserVoice will use reasonable efforts to make a change in the Service or recommend a commercially reasonable change to avoid processing by such Subprocessor. If UserVoice is unable to provide an alternative, Customer may terminate the effected Services. UserVoice will enter into written agreements with each Subprocessor containing reasonable

provisions relating to the implementation of technical and organizational measures in compliance with the GDPR. UserVoice will remain liable for acts and omissions of its Subprocessors in connection with the provision of the Services.

9. **TRANSFERS OUTSIDE OF THE EUROPEAN ECONOMIC AREA**

Customer acknowledges that UserVoice may, without Customer's prior written consent, transfer the Personal Data to a foreign jurisdiction provided such transfer is either (i) to a country or territory which has been formally recognized by the European Commission as affording the Personal Data an adequate level of protection or (ii) the transfer is otherwise safeguarded by mechanisms, such as Standard Contractual Clauses attached hereto as Schedule 1, and other certification instruments, recognized and approved by the European Commission from time to time.

UserVoice complies with the terms of the Privacy Shield Framework. Customer hereby acknowledges and agrees that on the request of the United States Department of Commerce (or any successor body) or a competent supervisory authority, enforcement or other public or regulatory authority, court or tribunal, UserVoice may make available to them a summary or representative copy of this DPA or any relevant provisions in the Service Agreement.

10. **INFORMATION OBLIGATIONS AND INCIDENT MANAGEMENT**

10.1. **Data Breach**. UserVoice will notify Customer of any Data Breach of which it becomes aware without undue delay, but no later than 72 hours, consistent with measures necessary to determine the scope of the breach and to restore the integrity of UserVoice's systems. UserVoice will use reasonable efforts to investigate the Data Breach and take any actions that are reasonably necessary to mitigate damage, as required by law and as appropriate under the circumstances.

10.2. **Notification**. UserVoice's notification of a Data Breach, to the extent known, will include: (a) the nature of the Data Breach; (b) the date and time upon which the Data Breach took place and was discovered; (c) the number of Data Subjects affected by the incident; (d) the categories of Personal Data involved; (e) the measures – such as encryption, or other technical or organizational measures – that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) the name and contact details of the data protection officer or other contact; and (g) a description of the likely consequences of the Data Breach.

10.3. **Coordination**. UserVoice will reasonably assist Customer in fulfilling its obligations to notify Data Subjects and the relevant authorities in relation to a Data Breach, provided that nothing in this section shall prevent either Party from complying with its obligations under Data Protection Laws. The Parties agree to coordinate in good faith on developing the content of any related public statements.

11. **OBLIGATIONS POST- TERMINATION**

Termination or expiration of this DPA shall not discharge the Parties from their obligations that by their nature may reasonably be deemed to survive the termination or expiration of this DPA.

12. **LIABILITY AND INDEMNITY**

Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Services Agreement.

13. **SEVERABILITY**

Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt in good faith to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this Agreement.

The Parties' authorized signatories have duly executed this DPA.

Signed	Signed Aaron Lapierre .....
for and on behalf of the Customer	for and on behalf of UserVoice, Inc.
Print Name:	Print Name: Aaron Lapierre .....
Title:.....	Title: Chief Customer Officer .....
Date:.....	Date: 09 / 03 / 2021 .....

SCHEDULE 1 - Standard Contractual Clauses (Controller to Processor)

SECTION I

Clause 1

Purpose and Scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1][1] for the transfer of personal data to a third country.

(b) The Parties:

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

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

HAVE AGREED to these Standard Contractual Clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.

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

Clause 2

Effect and invariability of the Clauses

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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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

Clause 3

Third-party beneficiary clause

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

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

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 1.B.

Clause 7

[Optional Clause Not Used]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.B, unless on further instructions from the data exporter.

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex 1.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1.B.

8.8 Onward Transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[2]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub- processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject. The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in this paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the

purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

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

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

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

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

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

Clause 15

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

15.1 Notification

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

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

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

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

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the

requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same

shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing Law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established. If the data exported is established outside of the EU Member States such dispute shall be resolved by the courts of the Republic of Ireland.

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

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

APPENDIX

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

1. Data exporter(s):

Name: **As set forth in the Agreement, DPA, and applicable Order into which these Clauses are incorporated.**

Address: **As set forth in the Agreement, DPA, and applicable Order into which these Clauses are incorporated.**

Contact person's name, position and contact details:

As set forth in the Agreement, DPA, and applicable Order into which these Clauses are incorporated.

Activities relevant to the data transferred under these Clauses:

The data exporter is transferring personal data for purposes of receiving the Box Service and any other additional services subscribed to, or licensed by, the data exporter.

Signature and date: **As per the signature and date of the Agreement entered into between the importer and exporter.**

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

2. Data importer(s):

Name: **UserVoice, Inc.**

Address: **234 Fayetteville Street, Raleigh, NC 27601**

Contact person's name, position and contact details: **Aaron Lapierre, Chief Customer Officer, privacy@uservoice.com**

Activities relevant to the data transferred under these Clauses: **The data importer is a provider of product feedback solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.**

Signature and date: **As per the signature and date of the Agreement entered into between the importer and exporter.**

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

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects Whose Personal Data is Transferred:

Data subjects include the individuals about whom UserVoice Processes data in connection with the UserVoice Services.

Categories of personal data transferred:

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

- Name
- Email Address
- IP Address
- Billing Address
- Company Name or Affiliation

Special categories of data transferred (if applicable):

Data relating to individuals provided to UserVoice in connection with the UserVoice Services, by (or at the direction of) Customer.

Frequency of the Transfer:

The frequency of the transfer is based upon the frequency at which the data exporter uploads Customer Personal Data (as defined in the Agreement) into the UserVoice Service. It is anticipated that transfers may be one-off in nature and/or continuous.

Nature of the Processing:

The purpose of the transfer and further processing is to provide the UserVoice Service pursuant to the Agreement, in accordance with the DPA, and as instructed by data exporter or data exporter's user(s) in their use of the UserVoice Service.

Purpose(s) of the Data Transfer and Further Processing:

UserVoice will process Customer Personal Data for the purposes of providing the UserVoice Services to Customer in accordance with the Addendum

Period for Which Personal Data Will be Retained:

Data importer will retain Customer Personal Data as stipulated in the Agreement and DPA and agreed by the Parties.

For Transfers to (Sub-)Processors, Specify Subject Matter, Nature, and Duration of the Processing:

As stipulated in the Agreement and DPA, and agreed by the Parties, Subprocessors and data exporter's affiliates may process and store Customer Personal Data in order to support and/or improve the UserVoice Service.

ANNEX II

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

The technical and organisational security measures implemented by the data importer are as described in the DPA.

ANNEX III - LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:
This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

Sub-processors including their location and services can be found on the UserVoice Subprocessor website found here: https://uservoice.com/security-compliance