DATA PROCESSING ADDENDUM
(GDPR & CCPA)

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Appcues Terms of Service, Appcues Master Subscription Agreement, or other written agreement between Appcues, Inc. ("**Appcues**") and the customer signatory (whether electronic or otherwise) to such agreement ("Customer," and each such agreement, the "**Agreement**") in each case where Appcues Processes any Customer Personal Data as part of performing Services for Customer under the Agreement. As to each Agreement, this DPA is coterminous with such Agreement and shall replace and supersede in its entirety any prior data processing agreement or similar document relating to Processing Customer Personal Data under such Agreement.

1. DEFINITIONS

1.1. "**Affiliate**" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with the applicable party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2. "**Authorized Affiliate**" means any Customer Affiliate that is (a) subject to Data Protection Laws and (b) permitted to use the Services under the Agreement.

1.3. "**CCPA**" means the California Consumer Privacy Act of 2018, including all laws and regulations implementing or supplementing CCPA.

1.4. "**Customer Personal Data**" means Personal Data agreed to be received or accessed and Processed by Appcues or a Sub-processor on behalf of Customer or an Authorized Affiliate pursuant to the Agreement, but excluding in all cases Prohibited Data.

1.5. "**Data Protection Laws**" means GDPR and CCPA, as and to the extent applicable.

1.6. "**EU-US Privacy Framework**" means the EU-US and Swiss-US Privacy Shield Frameworks and associated Principles, as applicable, and their respective successor frameworks, if any, as and when approved (or reinstated, as the case may be) by the European Commission, the UK Information Commissioner and/or the Swiss Federal Data Protection and Information Commissioner, as applicable, on the one hand, and the United States Department of Commerce on the other hand.

1.7. "**GDPR**" means the European Union ("EU") General Data Protection Regulation and all laws and regulations (including implementing laws and regulations) of the EU, the European Economic Area ("EEA") and their Member States ("EU GDPR"), as well as Switzerland under the Swiss Federal Data Protection Act ("Swiss FDPA") and, the United Kingdom under the United Kingdom Data Protection Act of 2018 and GDPR as incorporated into UK law ("UK GDPR"), the United Kingdom, in each case as and to the extent applicable to the Processing of Customer Personal Data under the Agreement and this DPA.

1.8. "**Prohibited Data**" means any data or information transmitted to Appcues other than directly through the Appcues API, as well as any data or information comprising (i) payment card or other payment method data or confidential financial information, (ii) health information, including without limitation "Protected Health Information" as that term is defined under the United States Health Insurance Portability and Accountability Act, (iii) "special categories" of personal data as described in GDPR Article 9, Paragraph 1, (iv) classified information under any applicable law, regulation or governmental authority, or (v) Personal Data of or relating to minors.

1.9. "**Restricted Transfer**" means (a) a transfer of Customer Personal Data from Customer or an Authorized Affiliate to Appcues or a Sub-processor, or (b) an onward transfer of Customer Personal Data from or between Appcues or a Sub-processor, in each of case (a) or (b) where such transfer is permitted under the Agreement but would be prohibited by GDPRData Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of GDPR) in the absence of a legal transfer mechanism to be established under this DPA.

1.10. "**Services**" means the products and/or services provided by Appcues under the Agreement.

1.11. "**Standard Contractual Clauses**" means (a) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); where the UK GDPR applies and the EU SCCs cannot legally be adopted as set forth in Section 8, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of UK GDPR ("UK SCCs"); and (iii) where the Swiss FDPA applies and the EU SCCs cannot legally be adopted as set forth in Section 8 (Restricted Transfers), the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("Swiss SCCs")agreement between Customer and Appcues set forth in Attachment 2 to this DPA, in each case if and to the extent applicable under Section 8 and as supplemented by the information contained in Attachments 1 to this DPA (Restricted Transfers). The EU SCCs, Modules Two and Three, are set forth in Attachment 2 to this DPA.

1.12. "**Sub-processor**" means any third party appointed by or on behalf of Appcues to Process Customer Personal Data on behalf of Appcues or any Appcues Affiliate.

The terms "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR; provided, however, that for purposes of CCPA, "**Data Subject**" shall be synonymous with "**Consumer**", and "**Personal Data**" shall be synonymous with "**Personal Information**", as those terms are defined in CCPA, and "**Supervisory Authority**" shall mean the Office of the Attorney General of the State of California, or its designee. The terms "**Commercial Purpose**", "**Sell**", and "**Service Provider**" shall have the same meanings as in CCPA.

2. APPLICABILITY; PROCESSING OF PERSONAL DATA

2.1. **Applicability.** This DPA applies only to the extent and as of the time the Data Protection Laws apply to Customer Personal Data and the Processing of such Customer Personal Data by Appcues or a Sub-processor under the Agreement.

2.2. **Authorization.** Customer authorizes and requests that Appcues Process Customer Personal Data as set forth in the Agreement and this DPA for the purposes set forth below. This DPA addresses (i) the subject-matter and duration of the Processing, (ii) the nature and

purpose of the Processing, and (iii) the types of Customer Personal Data, categories of Data Subjects whose Personal Data may be Processed and the obligations and rights of the parties.

2.3. Roles of the Parties.

The parties acknowledge and agree that with regard to the Processing of Customer Personal Data in connection with the Agreement and this DPA, as between the parties, Customer is either the Controller or a Processorand Data Exporter (even when acting as a Processor for a third-party Controller), and Appcues is in all cases a Processor, Data Importer and Service Provider, and Appcues may engage Appcues Affiliates or other Sub-processors pursuant to the requirements set forth in this DPA.

2.4. Customer's Obligations.

Without limiting any other obligations of Customer under the Agreement or this DPA, Customer shall:

a. Comply with all obligations under Data Protection Laws applicable to it, in particular with the principles relating to processing of Personal Data and the lawfulness of Processing, including obtaining and maintaining any required consent or other authorization from Data Subjects, as well as safeguarding the rights of Data Subjects in its use of the Services.

b. Promptly notify Appcues of any change in the applicability of Data Protection Laws to Customer or Customer Personal Data that may affect the Agreement or Appcues' ability to perform its obligations thereunder or under this DPA.

c. Serve as a single point of contact for Appcues and be solely responsible for the internal coordination, review and submission of instructions or requests of other Controllers that may permitted by Customer under the terms of the Agreement to use the Services. Appcues is discharged of any obligation to inform or notify such other Controllers when Appcues has provided applicable information or notice to Customer. Appcues is entitled to refuse any requests or instructions provided directly by a Data Controller that is not Customer.

2.5. Appcues' Obligations.

Without limiting any other obligations of Appcues under the Agreement or this DPA, Appcues shall:

a. Comply with all obligations under Data Protection Laws applicable to it.

b. Process Customer Personal Data on behalf of and in accordance with Customer's documented instructions as further specified in the Agreement and this DPA or as otherwise required or permitted under Data Protection Laws or as required by other applicable law or judicial process. Without limiting the foregoing, Appcues will not Sell Customer Personal Data and will not Process Customer Personal Data for its own or any other purposes (including any Commercial Purpose) except as otherwise expressly agreed in writing; provided, however, that Processing of Customer Personal Data by Appcues to ensure the security, operational maintenance, analysis, evaluation or development of the Services for the benefit of its customers without disclosing any Customer Personal Data and without having any adverse impact on the technical and organizational measures implemented by Appcues to protect Customer Personal Data shall not constitute processing for Appcues' own purposes.

c. Provide, at Customer's request and expense, reasonable cooperation and assistance in connection with Customer's obligations under Data Protection Laws as they relate to Customer Personal Data.

d. Without undue delay, inform Customer of any Personal Data Breach.

2.6. Purpose of Processing.

Customer instructs Appcues to Process Customer Personal Data for the following purposes: (i) Processing in accordance with the Agreement and any applicable purchase order or similar document; (ii) Processing initiated by Customer's authorized users (which may include authorized personnel of Customer's customers) in their use of the Services in accordance with Customer's configuration of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer via Appcues' support service where such instructions are consistent with the terms of the Agreement and applicable Data Protection Laws. Where an instruction cannot be followed due to the architecture of the Services or generates disproportionate efforts, Customer will reimburse Appcues for the costs arising from these efforts or Appcues may terminate all or applicable parts of the affected Services.

2.7. Further Details of Processing.

Further details of the Processing of Customer Personal Data, including, the categories of Customer Personal Data and Data Subjects are set forth in Attachment 1.

3. RIGHTS OF DATA SUBJECTS

3.1. Correction, Amendment and Deletion. To the extent Customer, in its use of the Services, does not have the ability to correct, amend, transfer or delete Customer Personal Data, as may be required by Data Protection Laws, Appcues shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Appcues is legally permitted to do so. Customer shall be responsible for any costs arising from Appcues' provision of such assistance to the extent legally permitted.

3.2. Data Subject Requests. Appcues shall, to the extent legally permitted, promptly notify Customer if it receives any complaint, notice or request from a Data Subject related to that person's Personal Data or either party's compliance with Data Protection Laws other than if provided as an instruction as set out in Section 2.6 (Purpose of Processing). Customer acknowledges that Appcues cannot verify the identity of a Data Subject (other than Customer personnel) as to any particular Customer Personal Data without Customer's assistance. Appcues shall not respond to any such Data Subject request except as required under Data Protection Laws, and Appcues shall provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request according to applicable Data Protection Laws, to the extent legally permitted and to the extent Customer cannot handle the request itself through its use of the Services. Customer shall be responsible for any costs arising from Appcues' provision of such assistance.

4. APPCUES PERSONNEL

4.1. Confidentiality. Appcues shall treat Customer Personal Data as Confidential Information under the Agreement and shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of the Customer Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Appcues shall ensure that such confidentiality obligations survive the termination of the personnel engagement. Appcues will promptly notify Customer if any Customer Personal Data is required by law or judicial process to be disclosed by it and will cooperate with Customer regarding the manner of such disclosure (but without prejudice to any obligation to comply with any such law or judicial process).

4.2. **Reliability.** Appcues shall take commercially reasonable steps to ensure the reliability of any Appcues personnel engaged in the Processing of Customer Personal Data.

4.3. **Limitation of Access.** Appcues shall ensure that Appcues' access to Customer Personal Data is limited to those personnel who require such access to perform the Agreement.

5. SUB-PROCESSORS

5.1. **General.** Except as set out in this Section 5, Appcues will not engage any Sub-processor to process Customer Personal Data without the prior written consent of the Customer.

5.2. **Appointment of Sub-processors.** Customer acknowledges, agrees and herewith consents that (a) Appcues Affiliates may act as Sub-processors; and (b) Appcues and Appcues Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. A current list of Sub-processors (and the subject matter, nature and duration of applicable Processing) is available upon Customer's request. In such cases Appcues will enter into a written agreement with the Sub-processor that will include contractual obligations substantially similar to those under this DPA relating to data protection, data security and the authorization of further sub-processors, in each case to the extent applicable.

The parties agree that copies of Sub-processor agreements provided to Customer by Appcues upon request may have all commercial information or clauses unrelated to data processing removed by Appcues beforehand.

5.3. **Liability.** To the extent required by applicable Data Protection laws, Appcues shall be liable for the acts and omissions of its Sub-processors to the same extent Appcues would be liable if performing the Services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5.4. **Changes to List of Current Sub-processors.** Appcues may remove, replace or appoint suitable and reliable further Sub-processors in its sole discretion. To the extent required under applicable Data Protection Laws Appcues will inform Customer about any changes to the list of Sub-processors in a timely fashion, which may be by announcing them to the Customer through automated notices. Customer may object to any change of Sub-processors in writing on legitimate grounds based on data protection or security concerns within 10 business days after receipt of Appcues' notice, and, if Customer so objects, Appcues will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Appcues is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable order document(s) in respect only to those Services which cannot be provided by Appcues without the use of the objected-to new Sub-processor, by providing written notice to Appcues. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

6. SECURITY

6.1. **Controls for the Protection of Personal Data.** Appcues shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Personal Data as set forth in the "Description of the technical and organizational security measures implemented by the data importer" as amended from time to time, a current copy of which is included as part of Attachment 1.

6.2. **Third-Party Certifications and Audits.** Upon Customer's written request at reasonable intervals, Appcues shall provide a copy of Appcues' then most recent third-party audits or certifications, as applicable, or any summaries thereof or other information that Appcues generally makes available to its customers at the time of such request evidencing Appcues' compliance with Section 6.1. In the absence of such audits or certificates, and to the extent Appcues is required to submit to audits under applicable Data Protection Laws, Customer may, at its own cost, audit the technical and organizational measures taken by Appcues.

6.3. **Audit restrictions**.

(a) Unless otherwise required by Data Protection Laws, Customer's audit right pursuant to Section 6.2 (Third-Party Certifications and Audits) is limited to once in any twelve-month period.

(b) An audit may not exceed three business days.

(c) Customer shall provide Appcues with at least 60 days' prior written notice (unless a Supervisory Authority or applicable Data Protection Law requires a shorter notice period).

(d) Customer and Appcues shall mutually agree the scope and determine the agenda of the audit in advance. The audit shall, to the extent possible, rely on certifications and audit reports or other verifications available to confirm Appcues' compliance with Section 6.1 and shall exclude any repetitive audits or requests for information.

(e) Customer shall conduct the audit under reasonable time, place and manner conditions and provide Appcues with a copy of the audit report and will inform Appcues without undue delay and comprehensively about any errors or irregularities related to Processing of Customer Personal Data detected during the audit.

(f) If an audit determines that Appcues is required to take corrective technical and/or organizational security measures, Appcues will at its sole discretion determine which measures are best suitable to ensure compliance and perform such measure within a reasonable time frame.

6.4. **Data Protection Checks by Supervisory Authorities.** Appcues will provide the Customer and Supervisory Authorities (as applicable) with all information and assistance reasonably necessary to investigate Personal Data Breaches or otherwise to demonstrate that the Services comply with Data Protection Laws to the extent that such inspections concern the Processing of Customer Personal Data under the Agreement, and will without undue delay implement the requirements of such Supervisory Authority in agreement with and at the cost of Customer.

7. RETURN AND DELETION OF PERSONAL DATA

At any time upon Customer's request, Appcues will return to Customer all Customer Personal Data and any copies thereof or will destroy all such Customer Personal Data and certify to Customer that it has done so, except to the extent Data Protection Laws or any other applicable law or judicial process imposed upon Appcues prevents it from doing so.

8. RESTRICTED TRANSFERS

8.1. EU-US Privacy Framework. During any period in which (i) the EU-US Privacy Framework is in effect and may legally serve as a valid data transfer mechanism under GDPR, and (ii) Appcues is certified in accordance with the requirements of such Framework, such Framework shall apply to any Restricted Transfer and the subsequent Processing of Customer Personal Data in connection with the Services to the fullest extent permitted by Data Protection Laws, and Appcues will comply with such Framework in connection with such Restricted Transfer and subsequent Processing.

8.2. Standard Contractual Clauses. Solely to the extent Section 8.1 does not apply to any Restricted Transfer due to the unavailability of the EU-US Privacy Framework or termination of such certification, Customer (as Controller under Module Two or as the transferring Processor under Module Three, but in either case as "data exporter") and Appcues and each Authorized Affiliate (each, as Processor under Module One or as the receiving Processor under Module Three, but in either case as "data importer") hereby enter into the Standard Contractual Clauses in respect of such Restricted Transfer; provided, however, that:

a. The Standard Contractual Clauses shall apply only to Customer Personal Data that is transferred from the EU, the European Economic Area and their respective Member States, the United Kingdom and/or Switzerland to the United States;

b. The Standard Contractual Clauses shall come into effect hereunder upon the commencement of the applicable Restricted Transfer; and

c. The terms and applicability of certain sections of the Standard Contractual Clauses shall be as follows:

i. Module Two (Controller to Processor) or Module Three (Processor to Processor) shall apply, as applicable to the actual role of Customer in connection with Restricted Transfers;

ii. Clause 7 (optional docking clause for third parties) shall be included and applied as may be agreed between the parties from time to time;

iii. Clause 9(a) (use of subprocessors - authorization), whether under Module Two or Module Three, shall be Option 2 of such Clause (general written authorization), and the applicable time period for notice therein shall be as set forth in Section 5.4 of this DPA;

iv. If Appcues has identified an independent dispute resolution body in its online Terms of Service (whether or not such online terms of service constitute the Agreement) or in its online Privacy Policy, and such body is eligible under the optional paragraph of Clause 11(a) (redress - dispute resolution), then such optional paragraph shall be included;

v. The version of Clause 13(a) (supervision - applicable Supervisory Authority) that applies to the role of Customer in connection with Restricted Transfers shall be included, and where, notwithstanding the provisions of such Clause 13(a), the parties may select the applicable Supervisory Authority, such Supervisory Authority shall be that of the Republic of Ireland;

vi. Except as otherwise expressly agreed in writing, Option 1 of Clause 17 (governing law - selected by the parties) shall apply, and the governing law under such Option shall be that of the Republic of Ireland;

vii. The applicable forum under Clause 18(b) (choice of forum and jurisdiction) shall be the Republic of Ireland; provided, however, that if Module Three applies and Customer is headquartered in the United States, then, subject to the rights of Data Subjects under Clause 18(c) (right of data subject to bring proceedings in the member state where the data subject resides), the forum shall be as set forth in the Agreement;

viii. The details required or permitted to be described in Annex I as to the parties and the description of the Restricted Transfer shall be as set forth in Attachment 1 to this DPA, and the competent Supervisory Authority shall be as set forth in Clause 13 (supervision - applicable Supervisory Authority) and Section 8.2(c)(v) above;

ix. The technical and organizational measures required or permitted to be described in Annex II shall be as set forth in the Agreement and in Attachment 1 to this DPA; and

x. The list of subprocessors required or permitted to be set forth in Annex III shall be as provided for in Section 8.2(c)(iii) and Section 5 of this DPA.

xi. Where the UK GDPR applies, then, notwithstanding the foregoing provisions of this Section 8.2 and to the extent legally permitted, (a) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to UK GDPR, and references to specific articles of "Regulation (EU) 2016/679" are replaces with the equivalent article or section of UK GDPR, (b) references to "EU," "Union," and "Member State" are replaced with "UK", and references to "competent supervisory authority" and "competent courts" shall be interpreted as references to the UK Information Commissioner and competent courts of England and Wales, (c) Clause 17 is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding 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.", (d) where the EU SCCs cannot lawfully be used, as modified above, under UK GDPR, the UK SCCs shall constitute part of this DPA and the relevant annexes or appendices of the UK SCCs shall be deemed completed with the information contained in Attachment 1 to this DPA, and (e) Part 2: Mandatory Clauses of the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as such Part 2 may be revised under Section 18 of those Mandatory Clauses, is hereby incorporated by reference into this DPA and shall take precedence over any conflicting terms of this DPA and Attachment 2 to this DPA; and

xii. Where the Swiss FDPA applies, then, notwithstanding the foregoing provisions of this Section 8.2 and to the extent legally permitted, (a) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to Swiss FDPA, (b) references to "EU," "Union," and "Member State" are replaced with "Switzerland", and references to "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland, (c) Clause 17 is replaced to state that "The Clauses are governed by the laws of Switzerland" and Clause 18 is replaced to state "Any dispute arising

from these Clauses shall be resolved by the courts of Switzerland. The parties agree to submit themselves to the jurisdiction of such courts.", and (d) where the EU SCCs cannot lawfully be used, as modified above, under Swiss FDPA, the Swiss SCCs shall constitute part of this DPA and the relevant annexes or appendices of the Swiss SCCs shall be deemed completed with the information contained in Attachment 1 to this DPA.

8.3. The parties agree that neither Section 8.1 nor Section 8.2 (if applicable) shall apply to a Restricted Transfer unless the effect of such Section, together with other reasonably practicable compliance steps undertaken by Appcues (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the Restricted Transfer to take place without breach of applicable Data Protection Law.

9. GENERAL TERMS

9.1. Governing Law and Jurisdiction. Without prejudice to the Standard Contractual Causes: (i) the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and (ii) this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

9.2. Order of Precedence. Nothing in this DPA reduces Appcues' or Customer's (or Customer Affiliates or their respective users') obligations under the Agreement or Applicable Data Protection Laws in relation to the protection of Customer Personal Data or permits any party to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the EU-US Privacy Framework or Standard Contractual Clauses, as applicable pursuant to Section 8, the EU-US Privacy Framework or Standard Contractual Clauses, as applicable, shall prevail.

9.3. Changed in Data Protection Laws. Either party may propose variations to this DPA if and as they may apply to a particular Data Protection Law, which such party believes in good faith are required as a result of any change in, or decision of a competent authority under, that Data Protection law. In the event of such a proposal, the parties agree to work together in good faith to implement mutually agreed changes. Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Appcues to protect Appcues and its Affiliates and Sub-processors against additional risks associated with such changes.

9.4. Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

_____ **Signature:** _____ **Printed Name:** _____ **Printed Title:** _____ **Signature Date:** _____ Signature: _____ Printed Name: _____ Printed Title: _____ Signature Date: _____ **Address for notices:**	**APPCUES, INC.** **Signature:** _____ **Printed Name:** _____ **Printed Title:** _____ **Signature Date:** _____ **Address for notices:** Appcues 177 Huntington Avenue Ste 1703 PMB 94414 Boston, MA 02115-3153 USA

ATTACHMENT 1

Certain Details of Processing of Customer Personal Data

Subject matter and duration of the Processing of Customer Personal Data
The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement (including ordering documents) and this DPA.

The nature and purpose of the Processing of Customer Personal Data
The nature and purpose of the Processing of the Customer Personal Data are set out in the Agreement and this DPA.

The types of Customer Personal Data to be transferred and Processed
Customer may submit Customer Personal Data (excluding special categories of data) to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- As to Customer personnel:
    - First and last name
    - Business email address or other business contact information
    - User ID
- As to other authorized users:
    - User ID
    - URL data

Sensitive data to be transferred
None.

The categories of Data Subjects to whom the Customer Personal Data relates
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer its sole discretion, and which may include, but is not limited to the following categories of Data Subjects:

- Customer personnel
- Other users authorized by Customer to use the Services in accordance with the Agreement

The period for which the Customer Personal Data will be retained
The period for which Customer Personal Data will be retained is set out in the Agreement and this DPA.

The obligations and rights of Customer and Customer Affiliates
The obligations and rights of Customer and Authorized Affiliates are set out in the Agreement and this DPA.

Description of the technical and organisational security measures

Within Appcues' area of responsibility, and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Appcues has in relation to the Customer Personal Data implemented will maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These include administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Personal Data including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, alteration, disclosure or access of or to Customer Personal Data. Appcues will not materially decrease the overall security of the Services during its provision of such Services to Customer.

To the extent that Appcues is certified to the following standards and/or controls, it shall adhere to and maintain such certification:

Statement on Standards for Attestation Engagements (SSAE) No. 16, System and Organization Controls for Service Organizations: Trust Services Criteria Type 2 report ("SOC 2, Type 2").

To demonstrate its commitment to trust and security, Appcues obtains relevant security certifications and undergoes regular testing and audits to ensure continued compliance. Appcues has completed a SOC 2 Type 2 audit that included Trust Services Principles of Security, Availability, Confidentiality with no exceptions. Our services undergo 3rd-party penetration testing on an annual basis. All of Appcues' data stores are backed up at least once every 24 hours. All backup data is encrypted. Appcues uses Amazon Web Services' High Availability feature that automatically provisions and maintains a synchronous standby replica in a different Availability Zone. Appcues is committed to the privacy of information. We use industry-leading encryption to protect all external traffic in transit (via HTTPS/TLS) and at rest (using AES-256 and an automated key rotation system).

ATTACHMENT 2

Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

STANDARD CONTRACTUAL CLAUSES

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] for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

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

[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.

add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3
Third-party beneficiaries

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

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

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4
Interpretation

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

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

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

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7 – Optional
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the

contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (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

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

8.9 Documentation and compliance

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

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

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

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[3].

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

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 rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller 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, they shall take due account of the state of the art,

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4]

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated

(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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] 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.[5] 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.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the

[5] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

controller. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.[6] 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

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

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

Clause 10
Data subject rights

MODULE TWO: Transfer controller to processor

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this

[6] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[7] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

[7] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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

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

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

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

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

Clause 12
Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13
Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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.

(a) [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.

(a) [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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these

Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

> (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
>
> (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[8];
>
> (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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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

[8] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

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

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

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

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] 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) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17
Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (specify Member State).]

[OPTION 2 (for Modules Two and Three): 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 _____ (specify Member State).]

Clause 18
Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

(b) The Parties agree that those shall be the courts of _____ (specify Member State).

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

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

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s):

The data exporter is the Customer identified in the Agreement or the applicable order documents. Customer's contact details (and that of its data protection officer, if any), role and and/or representative in the European Union, if any, are set forth in the applicable order documents.

Data importer(s):

The data importer is Appcues, and its role is that of processor (whether the data exporter is a controller or a processor). Appcues' contact details (and that of its data protection officer, if any) and/or representatives in the European Union, if any, are set forth in the Agreement or applicable order documents.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The description of the transfer is set forth in Attachment 1 to the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The applicable Supervisory Authority shall be determined pursuant to Section 8.2(c) of the DPA.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The technical and organisational measures implemented by the data importer are set forth on Attachment 1 to the DPA.

ANNEX III - LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Please see Section 5 and Section 8.2(c)(x) of the DPA.