Kajabi, LLC

Data Processing Addendum

Last Updated: September 16, 2020

1. **Introduction**.

   1.1. Application. Kajabi, LLC ("Kajabi") and Customer agree that this Kajabi Data Processing Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data and Personal Information in connection with the use of Kajabi's product and services by Customer. This DPA is incorporated by reference into the Kajabi Terms of Service ("Terms of Service). In the event of conflict or inconsistency between the terms set forth in this DPA and the Terms of Service, the DPA terms shall prevail.

   1.2. Precedence. The terms of this DPA supersede any contrary or conflicting provisions in the Kajabi Online Privacy Policy that may otherwise pertain to the processing of Customer Data and Personal Information, as they are defined herein.

   1.3. How to Execute this DPA:

      1.3.1. This DPA consists of two parts: the main body of the DPA and Attachments 1 and 2 (including Appendices 1 and 2).

      1.3.2. This DPAand the Standard Contractual Clauses in Attachment 2 have been pre-signed on behalf of Kajabi.

      1.3.3. To complete this DPA, Customer must: (i) complete the information in the signature and sign box on Page 9; and (ii) send the signed DPA to Kajabi by email to DPA@kajabi.com indicating, if applicable, the Customer's Account Number.

      1.3.4. Upon receipt of the validly completed DPA by Kajabi at this email address, this DPA will become legally binding.

      1.3.5. For the avoidance of doubt, Customer's signature of the DPA on page 9 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including the Appendices. If Customer wishes to separately execute the Standard Contractual Clauses and its Appendices, Customer should also complete the information in the signature box and sign on page 18.

   1.4. **Definitions**. A list of the defined terms used in this DPA is attached hereto as Attachment 1.

2. **General Terms**

   2.1. Scope. This DPA applies to the Product utilized by Customer. Data Protection Laws impose specific obligations on the Customer as a Controller and Kajabi as a Processor with regard to the processing of certain personal information processed as Customer Data. This DPA sets forth the data protection requirements imposed by Data Protection Law and as otherwise agreed to by Kajabi and Customer with respect to such personal information. This DPA does not apply to the processing of Service Generated Data, except in the limited circumstances where Service Generated Data contains Personal Information.

   2.2. Data Ownership. As between the parties, Customer retains all right, title and interest in Customer Data, and any rights not expressly granted in the Terms of Services or this DPA are reserved by Customer. The Customer acts as the Controller of Customer Data. Customer shall be responsible for complying with all requirements that apply to it under Data Protection Laws with respect to the processing of Personal Information and the processing instructions it gives to

Kajabi. This section does not affect Kajabi's rights in the technology, software, or services Kajabi licenses to Customer.

2.3. Permitted Processing.

2.3.1. Processing Instructions. Customer has contracted with Kajabi in order to benefit from the capabilities of Kajabi in securing and processing Customer Data for the purposes of providing the Product. Accordingly, Customer instructs Kajabi to process Customer Data, and in particular Personal Information, as necessary for the provision to Customer of the Product and as further instructed by Customer in its use of the Product. Kajabi shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, provided that all such discretion is compatible with the requirements of this DPA.

2.3.2. Legitimate Business Operations. Kajabi processes Customer Data in order to complete its legitimate business operations, which include primarily the delivery of the Product configured for use by Customer and its End Users. Additionally, Kajabi processes Customer Data in order to: (i) engage in providing customer service, troubleshooting, and support; (ii) ongoing improvement of the Product (including developing and providing new and improved features, productivity, reliability, and security); (iii) billing and account management; (iv) internal operations and reporting; (v) protecting against fraud, cybercrime, or illegal activity; (vi) evaluating performance; (vii) business modeling and forecasting; (viii) other legitimate business purposes that are consistent with the purposes stated herein.

2.4. Processing Restrictions. When processing Customer Data for its legitimate business operations (pursuant to Section 3.3.2), Kajabi will not use or otherwise process Customer Data or Personal Information for: (i) its own advertising or marketing purposes; (ii) End User profiling and inference association; or (iii) automated decision making.

2.5. Duration of Processing The duration of processing of Personal Information by Kajabi shall continue for the duration in which Customer purchases and uses the Product. Kajabi shall return Personal Information processed pursuant to this DPA following termination of the Customer's use of the Product or, to the extent permitted under applicable law, delete or destroy Personal Information in accordance with Industry Standards.

2.6. De-identified Information. Personal Information that has been de-identified in accordance with the requirements Data Protection Laws and is therefore not considered Personal Information ("De-Identified Information") is not subject to the provisions of the Terms of Service or this DPA. Kajabi may process Customer Data for the purpose of creating De-Identified Information, whether or not the De-Identified Information is to be used by Customer.

2.7. Confidentiality Commitment. Kajabi will ensure that its personnel engaged in the processing of Personal Information: (i) are informed of the Personal Information's confidential nature and use restrictions; (ii)have undertaken training on the privacy and data protection requirements relating to handling Personal Information and how it applies to their particular duties; and (iii) are aware both of Kajabi's duties and their personal duties and obligations under this DPA and Data Protection Laws.

3. Customer Obligations.

3.1. Customer is responsible for complying with the obligations of Data Protection Laws that apply to it as a Controller in respect of Personal Information processed using Kajabi's Product pursuant to the Terms of Service. Customer's obligations include, but are not limited to: (i) obtaining

parental consent for any End User's use of the Product that may be required by applicable law and communicating such consent and/or processing limitations to Kajabi; (ii) providing opt-in or opt-out notices and rights to End Users where processing of Personal Information is subject to such rights; (iii) providing all relevant notices to End User's required under Data Protection Laws; and (iv) deleting Personal Information as appropriate or required under Data Protection Laws.

3.2. Customer is responsible for evaluating the Product and determining whether they are appropriate for the processing and storage of Personal Information subject to any specific laws or regulations (including applicable Data Protection Laws) in a manner consistent with such laws. Kajabi is not responsible for compliance with any laws or regulations applicable to Customer and does not determine whether Customer Data includes information subject to general or specific regulation by any laws.

4. Disclosure of Processed Data.

4.1. Authorized Disclosures. Kajabi shall be permitted to collect, disclose, share, make available, or otherwise process Personal Information as necessary to provide the Product described in this DPA and the Terms of Service, provided that such processing does not violate Data Protection Laws.

4.2. Disclosure Restrictions. Kajabi will not disclose or provide access to Customer Data except: (i) as described in this DPA; (ii) as Customer directs; (iii) as required by law. In the event Customer Data is sought by law enforcement or legal process, Kajabi will attempt to direct the requesting party to contact Customer to request access or disclosure of the requested data directly from Customer. If compelled to disclose or provide access to Customer Data to law enforcement, Kajabi will notify Customer unless legally prohibited from doing so. If Kajabi receives a request from an individual or the individual's agent requesting access or modification to, or disclosure of, individual Personal Information, Kajabi will redirect the requesting party to make the request directly to Customer.

4.3. Disclosure to Subprocessors. Kajabi has engaged third parties to provide limited ancillary services on its behalf ("Subprocessors") and Customer consents to the disclosure of Personal Information to Kajabi's designated Subprocessors. Kajabi obtains reasonable assurances from the Subprocessors to provide a level of protection of Personal Information reasonable under the circumstances, taking into account the nature of the service provided by such Subprocessors and the nature of the Personal Information disclosed. Kajabi remains responsible for each Subprocessors compliance with its data protection obligations and for any acts or omissions of Subprocessors that cause Kajabi to breach its obligations under this DPA.

4.4. Kajabi may engage new Subprocessors from time to time. Kajabi will provide notice to Customer in the event a new Subprocessor is permitted to process Personal Information within 30 days prior to Kajabi providing the Subprocessor access to Personal Information. If Customer does not approve of the new Subprocessor, Customer must submit written notice to Kajabi before the end of the notice period and provide explanation for the reason for rejection of the proposed Subprocessor. Customer and Kajabi will work together in good faith to resolve Customer's objection to the use of the proposed Subprocessor. In the event the parties are unable to satisfactorily address Customer's objections, Kajabi may, in its sole discretion: (i) refrain from using the proposed Subprocessor to process Personal Information on behalf of Customer; (ii) terminate without penalty to Customer the part of Customer's subscription of the Services that relies on the processing by the proposed Subprocessor; or (iii) terminate, without penalty to Customer, Customer's entire subscription to the Services.

5. Data Security.

5.1. Safeguards. Kajabi will use reasonable and appropriate technical, administrative and organizational measures designed to ensure a level of confidentiality and security appropriate to the risks represented by the processing and the nature of Personal Information and to prevent unauthorized or unlawful processing of Personal Information, including but not limited to measures against accidental loss, disclosure or destruction of, or damage to, Personal Information. More information about Kajabi's data security safeguards can be found in our Security Statement, a copy of which can be obtained on request.

5.2. Data Security Certificates. Kajabi has obtained the third-party certifications and audits demonstrating compliance with industry standard data security frameworks and standards. Upon Customer's written request at reasonable intervals, and subject to Customer entering into a confidentiality agreement with Kajabi, Kajabi shall, to the extent that Kajabi is permitted to do so, make available to Customer that is not a competitor of Kajabi a copy of Kajabi's then most recent third-party audits or certifications, as applicable. Customer agrees that the provision of certification and audit reports to Customer pursuant to this DPA is sufficient to meet Kajabi's obligations with respect to compliance audits required by any Data Protection Laws. In the event the Data Protection Laws require audit of Kajabi's data security practices in addition to the furnishing of certifications and audit reports, Kajabi will work with Customer in good faith to comply with audit requirements legally compelled or required under Data Protection Laws.

5.3. Customer's Security Evaluation. Customer is solely responsible for determining whether the technical, administrative, and organizational measures for the Product described in this DPA and the related documentation, in addition to Kajabi's obligations under Data Protection Laws meet Customer's requirements. Customer acknowledges and agrees that security practices and policies implemented and maintained by Kajabi provide a level of security appropriate to the risk with respect to Personal Information. Kajabi is not responsible for Customer's compliance with Data Protection Laws nor does it or will it provide guidance to Customer with respect to the implementation of Customer's data security obligations.

5.4. Security Incident Notification.

5.4.1. Reporting Obligation. Kajabi shall notify Customer of any Information Security Incident promptly upon becoming aware of such Information Security Incident. Such notice shall summarize in reasonable detail the effect on Customer, if known, of the Information Security Incident and the corrective action taken or to be taken. Kajabi' obligation to report or respond to an Information Security Incident is not and will not be construed, in and of itself, as an acknowledgement by Kajabi of any fault or liability with respect to the incident.

5.4.2. Determination of Reportable Incident. Any determination regarding the applicability of Data Protection Laws to an Information Security Incident and the scope of the obligations of Kajabi pursuant to such laws shall be within the reasonable discretion of Customer. In the event Kajabi reasonably disagrees with any such determination in respect of any such Data Protection Laws that impose obligations directly or indirectly on Kajabi, Kajabi shall be entitled to make its own reasonable determination of such directly imposed obligations and act accordingly.

5.4.3. Investigation and Mitigation. In the event of an Information Security Incident, Kajabi shall:

5.4.3.1. Conduct a reasonable investigation of the reasons for and circumstances of the Information Security Incident;

5.4.3.2. Use best efforts and promptly take all necessary actions to rectify, prevent, contain and mitigate the impact of the Information Security Incident, and remediate the Information Security Incident;

5.4.3.3. Collect, preserve and document all evidence regarding the discovery and cause of, and vulnerabilities, response, remedial actions and impact related to the Information Security Incident using means that shall meet reasonable expectations of forensic admissibility; and

5.4.3.4. Provide reasonable assistance and cooperation as requested by Customer or Customer's designated representatives, in the furtherance of any correction, remediation, or investigation of any Information Security Incident or the mitigation of any damage.

5.4.4. Public Communications. The content of any filings, communications, notices, press releases, or reports related to any Information Security Incident that may, directly or indirectly, identify Customer or any of its officers, directors, employees, personnel, or reference Customer in connection with its consultants, agents, representatives, clients, customers, vendors, suppliers or service providers (other than Kajabi or Kajabi's Subprocessors) may request Customer's prior written approval, unless otherwise required by law, prior to any publication or communication thereof.

6. **Data Transfers**.

6.1. Cross-Border Data Transfers. Customer appoints Kajabi to transfer Personal Information to the United States or any other country in which Kajabi or its Subprocessors operate and to store Personal Information to provide the Product, except where otherwise described in this DPA. All transfers of Personal Information outside of the European Economic Area, the United Kingdom, and Switzerland to provide the Services shall be governed by the Standard Contractual Clauses in **Attachment 2**.

6.2. Privacy Shield. Kajabi is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Kajabi does not rely on the Privacy Shield Frameworks as a legal basis to transfer Personal Information as of July 16, 2020. Kajabi agrees to notify Customer if it determines that it is no longer able to provide the same level of protection as required by the Privacy Shield principles.

7. **Additional Regulations**.

7.1. Educational Institutions. In the event Customer is an educational institution or agency to which the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) applies, Kajabi shall be considered a "school official" for purposes of this DPA, as that term is defined under FERPA. Kajabi agrees to abide by the limitations imposed under FERPA with respect to school officials, so long as the Customer notifies Kajabi in advance of the processing of FERPA covered information.

7.2. Protected Health Information. Kajabi is not HIPAA compliant and currently we have no plans to become so. Accordingly, Customer may not use the Product to collect, store, or process any information of an individual that is covered by: (i) the Health Insurance Portability and Accountability Act; (ii) any applicable health or medical privacy regulation (whether state, federal, or local); or (iii) any other applicable law governing the processing, use, or disclosure of protected health information or medical information.

7.3. For California Resident's Personal Information. Notwithstanding Section 3.3, above, where Personal Information pertains to residents of the State of California, Kajabi shall not directly or indirectly: (i) sell Personal Information; (ii) retain, use, or disclose Personal Information for any purpose other than for the specific purpose of performing the Services; (iii) retain, use, or

disclose Personal Information for a commercial purpose other than providing the Product; or (iv) retain, use, or disclose Personal Information outside the direct business relationship between Customer and Kajabi. Kajabi certifies that it understands these restrictions and will comply with them.

7.4. GDPR. To the extent that Kajabi is a processor or subprocessor of Personal Information subject to the GDPR, Kajabi agrees that the following terms ("GDPR Terms") apply to the processing of Personal Information (as defined by the GDPR), within the scope of the GDPR, by Kajabi as a processor to Customer. For the avoidance of doubt, the GDPR Terms do not apply where Kajabi is the data controller.

7.4.1. Kajabi shall:

7.4.1.1. process the Personal Information only on documented instructions from Customer, including with regard to transfers of Personal Information to a third country or an international organization, unless required to do so by Union or Member State law to which Kajabi is subject; in such a case, Kajabi shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

7.4.1.2. ensure that persons authorized to process the Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

7.4.1.3. take all measures required pursuant to Article 32 of the GDPR;

7.4.1.4. respect the conditions referred to in the Article 28(2) through (4) for engaging another processor;

7.4.1.5. taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

7.4.1.6. assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Kajabi;

7.4.1.7. at the choice of Customer, delete or return all the Personal Information to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Information;

7.4.1.8. make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

7.4.1.9. immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

7.4.2. Where Kajabi engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection

obligations, Kajabi shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

7.4.3. 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, Customer and Kajabi shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

7.4.3.1. the pseudonymisation and encryption of Personal Information;

7.4.3.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

7.4.3.3. the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and

7.4.3.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. (Article 32(1))

7.4.4. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information transmitted, stored or otherwise processed. (Article 32(2))

7.4.5. Customer and Kajabi shall take steps to ensure that any natural person acting under the authority of Customer or Kajabi who has access to Personal Information does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4).

7.4.6. Kajabi shall notify Customer without undue delay after becoming aware of a Personal Information breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Kajabi.

9. **Contact**. Customer may contact Kajabi regarding this DPA or any of its privacy and security commitments by emailing Privacy@Kajabi.com or mailing us at:

   Kajabi, LLC
   ATTN: Data Protection Officer
   17100 Laguna Canyon Road, Suite 100

   Irvine, CA 92603

10. **Legal Effect**. This DPA shall only become legally binding between Customer and Kajabi when the formalities set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

List of Attachments

Attachment 1: Definitions

Attachment 2: Standard Contractual Clauses

[Signature page follows]

[Signature page to DPA]

The parties' authorized signatories have duly executed this DPA:

KAJABI, LLC

Signature: Ahad Khan

Name: Ahad Khan

Title: Chief Financial Officer

Date: 9/16/20

CUSTOMER:

Signature: _____

Customer Legal Name: _____

Pring Name: _____

Title: _____

Date: _____

Attachment 1

Definitions

1. Capitalized terms used but not defined in this DPA will have the meanings provided in the Kajabi Terms of Service. The following defined terms are used in this DPA:

   1.1. "**Controller"** means: (i) the entity that determines the purposes and means of processing the Processing of Personal Information; and (ii) a "business" (as defined under the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, et seq., *as amended*).

   1.2. "**Customer**" means the person or entity purchasing Kajabi's Services.

   1.3. "**Customer Data**" means all information or data, electronic or otherwise, that are provided to Kajabi by, or on behalf of Customer through the use of the Product.

   1.4. "**Data Protection Laws**" means all laws and regulations, including laws and regulations of the United States and its states, applicable to the processing of Personal Information pursuant to the Terms of Service.

   1.5. "**End User**" means any individual or entity that directly or indirectly through another user: (a) accesses or uses the Customer's software, data, text, audio, video, or images (i.e. Customer's content); or (b) otherwise accesses or uses the Product under a Customer's account. The term "End User" does not include individuals or entities when they are accessing or using the Product or any content under their own account or separate and apart from Customer, rather than under Customer's account.

   1.6. "**GDPR**" means 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

   1.7. "**Industry Standards**" means industry standards that are reasonable and appropriate to the nature of the Personal Information being processed in this DPA, and takes into account the standards and practices employed by Kajabi's peers, for the industry in which Kajabi operates relating to the privacy, confidentiality or security of Personal Information, as updated from time to time.

   1.8. "**Information Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Information while processed by Kajabi.

   1.9. "**Personal Information**" means (i) any information relating to an identified or identifiable natural person; and (ii) "personal data" as defined in the GDPR, where such information is Customer Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

   1.10. "**Service Generated Data**" means data generated or derived by Kajabi through the operation of the Product. Service Generated Data does not include Customer Data.

   1.11. "**Standard Contractual Clauses**" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European

Commission decision 2010/87/EC, dated 5 February 2010. The Standard Contractual Clauses are in Attachment 2.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms "data importer" and "data exporter" have the meanings given in the Standard Contractual Clauses.

Attachment 2

The Standard Contractual Clauses (Processors)

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

The entity identified as "Customer" in the DPA

(the "**data exporter**")

and

Kajabi, LLC

17100 Laguna Canyon Road, Suite 100, Irvine, CA 92603

(the "**data importer**")

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

Definitions

Clause 1: Definitions

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

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

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

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

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

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

Clause 2: Details of the transfer

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

Clause 3: Third-party beneficiary clause

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

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

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

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

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6: Liability

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

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

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue

a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

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

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

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

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

Clause 8: Cooperation with supervisory authorities

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

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

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

Clause 9: Governing Law.

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

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[Signature page follows]

[Signature page of Standard Contractual Clauses]

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

On behalf of the data importer:

Name (written out in full): Ahad Khan

Position: Chief Financial Officer

Address: 17100 Laguna Canyon Road, Ste. 100, Irvine, CA 92603

Signature: Ahad Khan

Appendix 1 to the Standard Contractual Clauses

Data exporter: The data exporter is the entity identified as the Customer in the DPA.

Data importer: The data importer is Kajabi, LLC, a provider of online services.

Data subjects: Data subject include the following categories of users:

- Customer's End Users;
- Data exporter's representatives, including current and former employees, contractors, collaborators, and customers;
- Minors
- Data Exporter's service provider or professional advisors who interact with the Services.

Categories of data: The personal data transferred that is included in an electronic form in the context of the Services. Depending on Customer's use of the Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Personal contact information (for example, name, email address, mailing address, phone number, user name, gender, date of birth) ;
- Account authentication data (for example user name, password or PIN code, security question, audit trail);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing history, search history, clicks, analytics data);
- Device identification (for example MAC address IMEI-number, SIM card number,);
- Unique identification numbers and signatures (for example IP addresses, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Financial information (for example, bank account name and number, credit card name and number, payment behavior, creditworthiness);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

The processing operations are defined in Section 3 of the DPA.

Appendix 2 to the Standard Contractual Clauses

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

1. **Personnel**. Data importer's personnel will not process Customer Data or personal data without authorization. Personnel are obligated to maintain the confidentiality of any such Customer Data and personal data and this obligation continues even after their engagement ends.

2. **Data Privacy Contact.** The data privacy officer of the data importer can be reached at the following address:

Kajabi, LLC

17100 Laguna Canyon Road, Suite 100,

Irvine, CA 92603

3. **Technical and Organization Measures.**

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