Kajabi, LLC

Data Protection Addendum

Effective Date: September 27, 2021

Last Updated: September 27th, 2021

This Data Protection Addendum ("DPA") supplements the Kajabi Terms of Service Agreement between Customer and Kajabi, LLC ("Kajabi") into which it is incorporated by reference (hereinafter, the "Agreement").

1. **Introduction**.

1.1. Definitions. Capitalized terms used but not defined in this DPA will have the meanings provided in the Kajabi Agreement. The following defined terms are used in this DPA:

(a) "Customer" means the person or entity purchasing Kajabi's Product.

(b) "Customer Account Data" personal data that relates to Customer's relationship with Kajabi, including the names or contact information of individuals authorized by Customer to access Customer's account. It also includes billing and payment information of individuals that Customer has associated with its account.

(c) "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. Customer Data includes Customer's Content, as defined in the Agreement.

(d) "Data Protection Law" means all laws, legislation, regulations, judicial or regulatory actions, as now or as may become effective, applicable to the processing of Personal Data pursuant to the Agreement.

(e) "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).

(f) "Industry Standards" means industry standards that are reasonable and appropriate to the nature of the Personal Data 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 Data, as updated from time to time.

(g) "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 Data while processed by Kajabi.

(h) "Personal Data" means (i) any information relating to an identified or identifiable natural person (a "data subject"), 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.

(i) "Product" has the same meaning as set forth in the Agreement.

(j) "Product Generated Data" means data generated or derived by Kajabi through the operation of the Product. Product Generated Data does not include Customer Data.

(k) "Standard Contractual Clauses" means, depending on the circumstances unique to the Customer, any of the following:

- EU Standard Contractual Clauses approved by the European Commission in decision 2021/914, whether they be "Controller-to-Processor" or "Controller-to-Controller."
- UK Standard Contractual Clauses, whether they be "Controller-to-Processor" or "Controller-to-Controller."

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.

2. **General Terms**

2.1. Scope and Precedence. The parties agree that this DPA sets forth their obligations regarding the processing of Customer Data, Customer Account Data, and Personal Data in connection with Customer's purchase and use of the Product. This DPA does not apply to the processing of Product Generated Data, except in the limited circumstances where Product Generated Data contains Personal Data. In the event of any conflict or inconsistency between the terms of this DPA terms and any other terms in the Agreement, the terms in the DPA shall prevail. The terms of the DPA supersede any conflicting provisions of the Kajabi Privacy Policy that otherwise may apply to processing of Customer Data, Customer Account Data, or Personal Data as defined herein. For clarity, the Standard Contractual Clauses prevail over any other term of the DPA.

2.2. Relationship of the Parties. The parties acknowledge and agree that, as between the parties:

(a) As to Customer Data. Customer may act as a controller or processor and Kajabi is a processor. Kajabi will process Customer Data in accordance with Customer's processing instructions as set forth in Section 2.3 of this DPA. Customer shall be responsible for complying with all requirements that apply to it under Data Protection Law with respect to the processing of Personal Data and the processing instructions it gives to Kajabi. Customer retains all right, title and interest in Customer Data, and any rights not expressly granted in the Agreement or this DPA are reserved by Customer. This section does not affect Kajabi's rights in the technology, software, or services Kajabi licenses to Customer.

(b) As to Customer Account Data. With regard to Customer Account Data, Kajabi is a an independent (not joint) controller with Customer. Kajabi will process Customer Account Data as a controller in order to carry out its Legitimate Business Operations as set forth in

Section 2.3.2 of this DPA and in accordance with this DPA, the Agreement, and the Kajabi Privacy Policy.

(c) As to Product Generated Data. With regard to the processing of Product Generated Data, Customer may act either as a controller or processor and Kajabi is an independent (not joint) controller with Customer. Kajabi will process Product Generated Data as a controller in order to carry out its Legitimate Business Operations as set forth in Section 2.3.2 of this DPA and in accordance with this DPA, the Agreement, and our Privacy Policy.

2.3. Permitted Processing.

(a) 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 Data within Customer Data, 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.

(b) Legitimate Business Operations. Kajabi processes Customer Data, Customer Account Data, and Product Generated 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 and 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.

(c) Processing Limitations. Kajabi will processing Personal Data in order to provide the Product and as further instructed by Customer in its use of the Product, for example through Customer's Product configurations, settings, add-ons, integrations, designs, and preferences. Schedule 1 (Details of Processing) of this DPA provides further details on the processing details.

3. **Customer Obligations**.

3.1. Customer is responsible for complying with the obligations of Data Protection Law that apply to it as a controller or processor in respect of Personal Data processed using Kajabi's Product pursuant to the Agreement. Customer's obligations include, but are not limited to: (i) obtaining 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 Data is subject to such rights; (iii) providing all relevant notices to end user's required under Data Protection Law; and (iv) deleting Personal Data as appropriate or required under Data Protection Law. Customer will ensure that its processing instructions comply with applicable Data Protection Law. Customer acknowledges that Kajabi is neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Kajabi's provision of the Product meets or will

meet the requirements of such laws or regulations. Customer will ensure that Kajabi's processing of Customer Data, when done in accordance with Customer's processing instructions, will not cause Kajabi to violate any applicable law or regulation, including applicable Data Protection Law. Kajabi will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate any applicable law or regulation, including applicable Data Protection Law.

3.2. Customer is responsible for evaluating the Product and determining whether it (and its individual features) are appropriate for the processing and storage of Personal Data subject to any specific laws or regulations (including applicable Data Protection Law) in a manner consistent with such laws or regulations.

4. Roles and Responsibilities.

4.1. Data Subject Rights Requests; Assistance. Customer is responsible for responding to all requests from Customer's data subjects regarding their rights under Data Protection Law including, where necessary, using Product functionality. Kajabi will assist Customer, in a manner consistent with Product functionality and its role as a processor of Personal Data for Customer, in fulfilling data subject requests to exercise their rights to access, delete, rectify, or restrict their Personal Data under Data Protection Law. Should Kajabi receive a request directly from a data subject or their agent to exercise on or more of the data subject's rights under Data Protection Law in connection with Customer's use of the Product, Kajabi shall direct the data subject to make the request directly to Customer.

4.2. Data Retention and Deletion. Kajabi will provide to Customer, as part of the functionality of the Product, the ability to access, download, extract, and delete Customer Data stored within the Product. Except for trial offers periods, Kajabi will retain Customer Data that remains stored in the Product in a limited function for 90 days after the expiration or termination of Customer's right to use the Product. After such 90 day period, Kajabi shall delete all Customer Data (including any Personal Data contained within Customer Data), unless Kajabi is permitted or required by applicable law, or otherwise agrees, in its sole discretion, to maintain Customer Data upon request from Customer.

4.3. Compliance with Data Protection Law. Customer and Kajabi each understand Data Protection Law may require the collection, maintenance, and disclosure of certain information related to compliance with Data Protection Law. Customer and Kajabi each agree maintain and keep up-to-date all information required to be maintained under Data Projection Laws, and to make such information available to the other party where requested. Kajabi (including its authorized representatives) will reasonably cooperate, upon request, with supervisory authorities (as defined in the applicable Data Protection Law) in the performance of its tasks.

4.4. Impact Assessments and Consultations. Kajabi will provide reasonable cooperation to Customer in connection with any data protection impact assessment and any consultation with regulatory authorities required by applicable Data Protection Law. Kajabi is entitled to seek additional compensation from Customer for cooperation with requests which would impose costs or efforts on Kajabi which are unreasonable given the circumstances and may, in its sole discretion, deny such requests.

5. Disclosure of Processed Data.

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

5.2. 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.

5.3. 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 Data to Kajabi's designated Subprocessors. Kajabi obtains reasonable assurances from the Subprocessors to provide a level of protection of Personal Data reasonable under the circumstances, taking into account the nature of the service provided by such Subprocessors and the nature of the Personal Data 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. Customer consents to Kajabi engaging additional third party sub-processors to process Customer Data within the Product for Legitimate Business Operations provided that Kajabi maintains an up-to-date list of its sub-processors which is available upon request and subject to Customer agreeing to confidentiality provisions.

5.4. Engagement of Additional Subprocessors. Kajabi may engage new or replace Subprocessors from time to time. Kajabi will provide notice to Customer in the event a new Subprocessor is permitted to process Personal Data within 30 days prior to Kajabi providing the Subprocessor access to Personal Data. 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 Data on behalf of Customer; (ii) terminate without penalty to Customer the part of Customer's subscription of the Product that relies on the processing by the proposed Subprocessor; or (iii) terminate, without penalty to Customer, Customer's entire subscription to the Product.

6. **Data Security**.

6.1. 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 Data and to prevent unauthorized or unlawful processing of Personal Data, including but not limited to measures against accidental loss, disclosure or destruction of, or damage to, Personal Data. More information about Kajabi's data security safeguards can be found in Schedule 2.

6.2. Data Security Review. Kajabi conducts regular testing and assessment of its technical and organizational measures for purposes of evaluating their effectiveness. In the event the Data Protection Law require audit of Kajabi's data security practices, Kajabi will work with Customer

in good faith, and subject to reasonable confidentiality controls, to comply with audit requirements legally compelled or required under Data Protection Law.

6.3. 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 Law 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 Data. Kajabi is not responsible for Customer's compliance with Data Protection Law nor does it or will it provide guidance to Customer with respect to the implementation of Customer's data security obligations. Customer is further responsible for using features and functionalities made available by Kajabi to maintain appropriate security in light of the nature of Customer Data processed as a result of Customer's use of the Product.

6.4. Security Incident Notification.

(a) 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.

(b) Determination of Reportable Incident. Any determination regarding the applicability of Data Protection Law 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 Law 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.

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

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

ii. 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;

iii. 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

iv. 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.

(d) 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.

7. **International Provisions**

7.1. Location of Processing. Customer acknowledges that, as of the Effective Date, Kajabi primarily processes Personal Data in the United States of America.

7.2. Jurisdiction Specific Terms. To the extent Kajabi processes personal data originating from and protected by applicable Data Protection Law in one of the jurisdictions listed in Schedule 3 (Jurisdiction Specific Terms) of this DPA, the terms specified in Schedule 3 with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

7.3. Cross Border Data Transfer Mechanisms for Data Transfers. To the extent Customer's use of the Product requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area ("EEA"), the United Kingdom, Switzerland, or any other jurisdiction listed in Schedule 3 to Kajabi located outside of that jurisdiction ("Transfer Mechanism"), the terms set forth in Schedule 4 (Cross Border Transfer Mechanisms) will apply.

8. **Failure to Perform.** In the event that changes in law or regulation render performance of this DPA impossible or commercially unreasonable, the parties may renegotiate this DPA in good faith. If renegotiation would not cure the impossibility or the parties cannot reach an agreement, the parties may mutually agree to terminate the Agreement for convenience.

9. **Updates.** Kajabi may update the terms of this DPA from time to time; provided, however, Kajabi will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in a Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to the Product.

10. **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, #100
Irvine, CA 92603

Schedule 1

Details of Processing

1. **Nature and Purpose of the Processing.** Kajabi will processing Personal Data as necessary to provide the Product pursuant to the Agreement.

2. **Processing Activities.**

   2.1. For Customer Data: Kajabi will process Customer Data to conduct its Legitimate Business Operations as well as the following activities (which may also be considered Legitimate Business Operations:

   - Delivery of the functional capabilities of the Product as licensed, configured, and used by Customer and its end users;
   - Troubleshooting;
   - Preventing, detecting, and remediating issues with the Product or Customer's or end user's use of the Product;
   - Auditing the use of the Product;
   - Ongoing improvement to the Product and Kajabi's customer services.

   2.2. For Customer Account Data and Product Generated Data: Kajabi will process Customer Data to conduct its Legitimate Business Operations as well as the following activities (which may also be considered Legitimate Business Operations:

   - Accounts and record services, including billing and account management;
   - Administration services, including customer support, troubleshooting, and administrative assistance;
   - Fraud and crime prevention, including preventing cybercrime or cyberattacks;
   - Improving functionality of the Product or Kajabi's customer services;
   - Internal operations related to account management, employee compensation, partner compensation, business modeling, reporting, financial reporting, and legal compliance.

3. **Duration of Processing.** The duration of processing of Customer Data by Kajabi shall be for the duration in which Customer purchases and uses the Product. Kajabi shall return Customer Data 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 Customer Data in accordance with industry standards.

4. **Categories of Data Subjects.** The Personal Data transferred concern the following categories of data subjects:

4.1. For Customer Data: Customer's end users.

4.2. For Customer Account Data: Customer's employees, staff, and individuals authorized by Customer to access Customer's Account or make use of the Product on Customer's behalf.

4.3. Product Generated Data: Customer and Customer's end users.

5. Categories of Personal Data. The following is a list of data categories processed by Kajabi:

5.1. For Customer Data: Personal Data contained in Customer Data. Such data may include:

- 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.

5.2. For Customer Account Data:

- Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, sex, and employment affiliation.
- Employment details, including information relating to the employment of the data subject, including employment affiliation.
- Financial details, including payment information related to the provision of the Product.
- Goods or services provided and related information, including details of the goods or services supplied, licenses issued, and contracts with Kajabi.

5.3. For Product Generated Data: Data on the location of the device generated in the context of providing the Product, and the date, time, duration and the type of communication and activity logs used to identify the source of requests, optimize and maintain performance of the Product, and investigate and prevent system abuse.

6. Special Data Categories. The following special data categories may be processed by Kajabi. As used herein, "special data categories" means any Personal Data or that falls within the definition of "special categories of data" under GDPR or any other applicable law or regulation relating to privacy and data protection.

6.1. For Customer Data: Special data categories may, from time to time, be processed where Customer or its end users choose to include such data within the communications or information that are transmitted using the Product. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Customer's end users to transmit or process, any special data categories.

6.2. For Customer Account Data and Product Generated Data: Special data categories are not contained in Customer Account Data or Product Generated Data.

Schedule 2

Technical and Organizational Security Measures

A description of the technical and organizational security measures implemented by Kajabi is included as follows. Where applicable, this Schedule 3 shall serve as Annex II to the Standard Contractual Clauses.

Measures of pseudonymisation and encryption of personal data:	● Personal data is encrypted in transit, at rest and protected by role-based access controls.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:	● Kajabi ensures that user data access is restricted to business responsibilities or tasks based (i.e., Human Resources is the only team with access to HR data)
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:	● Kajabi ensures that all backups are regularly analyzed for successful recovery.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing:	● Kajabi ensures effectiveness of technical and organizational measures via internal and external assessments.
Measures for user identification and authorisation:	● Users are required to authenticate via a password. ● Internal users access is role-based and leverages multi-factor authentication where possible.
Measures for the protection of data during transmission:	● Kajabi encrypts data in transit using secure SSL/TLS cryptographic protocols. ● Implementation of firewalls to secure networks.
Measures for the protection of data during storage:	● Physical and infrastructure security. ● Implementation of firewalls to secure networks. ● Protection against viruses, worms, and other data corruption threats.
Measures for ensuring physical security of locations	

at which personal data are processed:	● Kajabi utilizes subproccesors to store personal data. This data is widely held off site at different data centers throughout the country. These data centers have rigorous physical security controls in place, including but not limited to access control, monitoring, entry points, CCTV and intrusion detection. Kajabi reviews these controls regularly.
Measures for ensuring events logging:	● Kajabi ensures that event logging covers the following activities: user activity, administrator and privileged user activity, processing activity, network and firewall activity, audit activity, and scanning.
Measures for ensuring system configuration, including default configuration:	● Any computer or network devices utilized by Kajabi implement a baseline configuration that includes but is not limited to: ○ removing and disabling unnecessary user accounts; ○ changing default or guessable account passwords to something non-obvious; ○ authenticating users before enabling internet-based access to sensitive data, or data critical to Kajabi
Measures for internal IT and IT security governance and management:	● In order to ensure internal and IT security governance and management, Kajabi has developed an organization-wide information security policy, as well as enabled all employees to be knowledgeable about their role and responsibilities. Kajabi also ensures that legal and regulatory requirements are reviewed regularly.
Measures for certification/assurance of processes and products:	● In order to maintain certification/assurance of processes and products, Kajabi continues to maintain data governance. Kajabi ensures that rules for consent, data subject requests and managing data subject complaints are defined. ● Kajabi engages in external reviews and assessments to further validate implemented measures.
Measures for ensuring data minimisation:	● Kajabi ensures that only relevant and necessary information required is processed.
Measures for ensuring data quality:	

	● Data that is processed is monitored to ensure it is accurate, complete and reliable.
Measures for ensuring limited data retention:	● Kajabi Customers determine what Member Data they route through the Kajabi Services and how the Kajabi Services are configured. ● If a Customer is unable to delete their Member Data, then Kajabi deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Processing Addendum and in accordance with Applicable Data Protection Law.
Measures for ensuring accountability:	● Kajabi will continue to ensure accountability. Kajabi takes responsibility for complying with the UK GDPR, at the highest management level and throughout our organization ● We put in place appropriate technical and organizational measures, such as: ○ Adopting and implementing data protection policies; ○ Maintaining documentation of our processing activities; ○ Implementing appropriate security measures; ○ Carrying out data protection impact assessments for uses of personal data where necessary; ○ Appointing a data protection officer (where necessary); ● Kajabi reviews and updates our accountability measures at appropriate intervals.
Measures for allowing data portability and ensuring erasure:	● Data subjects have the right to receive the personal data concerning them, which they have provided to a controller. Data subjects may request any and all personal data concerning them that they have provided to a controller to be erased.
Additional Measures	● Kajabi implements the following (but not limited to) technical and organizational measures: ○ maintaining information security policies and regularly reviewing as necessary;

- system and event logging and other related monitoring procedures have been enabled;
- establishing a patch management and vulnerability management program;
- appointing a Data Protection Officer (DPO)

Supplemental Safeguards

- With respect to Cross-Border Data Transfers pursuant to Standard Contractual Clauses only, Kajabi offers the following supplemental safeguards:
  - If Kajabi receives a valid and binding order from any governmental body for disclosure of its Personal Information, Kajabi will use every reasonable effort to redirect the requesting party to request the Personal Information directly from Customer.
  - Kajabi shall take no voluntary action pursuant to U.S. Executive Order 12333.
  - Kajabi will truncate, hash, or encrypt Personal Information in transit from the European Economic Area.
  - Kajabi will publish a transparency report indicating the types of binding legal demands for the Personal Information it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702.

Schedule 3

Jurisdiction Specific Terms

1. California.

1.1. The definition of "Data Protection Law" will include the California Consumer Privacy Act (CCPA).

1.2. The following definitions are amended:

1.2.1. The definition of "Personal Data" includes "Personal Information" as defined in the CCPA.

1.2.2. The definition of "controller" includes "Business" as defined in the CCPA.

1.2.3. The definition of "processor" includes "Service Provider" as defined in the CCPA.

1.2.4. Where the term "data subject" is used in the DPA, it shall include "Consumer" as defined by the CCPA. Any data subject rights described in the DPA apply to Consumer rights. Customer is aware that Kajabi is not able to verify requests from Customer's Consumers or Consumers' agents on behalf of Customer.

1.3. Kajabi will process, retain, use, and disclose personal data only as necessary to provide the Product pursuant to the Agreement, which constitutes a business purpose. Kajabi agrees not to (a) sell (as defined by the CCPA) Customer's personal data or Customer end users' personal data; (b)retain, use, or disclose Customer's personal data for any commercial purpose (as defined by the CCPA) other than providing the Product; or (c) retain, use, or disclose Customer's Personal Data outside of the scope of the Agreement. Kajabi understands its obligations under the Applicable Data Protection Law and will comply with them.

1.4. Kajabi certifies that its sub-processors, as described in Section 5.3 of this DPA, are Service Providers under CCPA, with whom Kajabi has entered into a written contract that includes terms substantially similar to this DPA.

1.5. Kajabi will implement and maintain reasonable security procedures and practices appropriate to the nature of the personal data it processes as set forth in Section 6 (Security) of this DPA.

2. **European Economic Area (EEA)**.

2.1. The definition of "Applicable Data Protection Law" includes the General Data Protection Regulation (EU 2016/679) ("GDPR").

2.2. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

3. **United Kingdom (UK)**

3.1. References in this DPA to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

3.2. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.

4. **Canada**.

4.1. The definition of "Applicable Data Protection Law" includes the Federal Personal Data Protection and Electronic Documents Act (PIPEDA).

5. Australia.

5.1. The definition of "Applicable Data Protection Law" includes the Australian Privacy Principles and the Australian Privacy Act (1988).

5.2. The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Law.

5.3. The definition of "Sensitive Data" includes "Sensitive Information" as defined under Applicable Data Protection Law.

Schedule 4

Cross-Border Transfer Mechanisms

,For data transfers that are subject to Standard Contractual Clauses, the Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) as follows:

1. **For Transfers from the European Economic Area or Switzerland**

   1.1. Attachment 1: (Module 1: (Controller to Controller) of the Standard Contractual Clauses approved by the European Commission in decision 2021/914 will apply where Kajabi is processing Customer Account Data and Product Generated Data associated with Customer's end users.

   1.2. Attachment 2: (Module 2: (Controller to Processor) of the Standard Contractual Clauses approved by the European Commission in decision 2021/914 will apply where Customer is a controller of Customer Data and Kajabi is processing Customer Data.

   1.3. Attachment 3: (Module 3: (Processor to Processor) of the Standard Contractual Clauses approved by the European Commission in decision 2021/914 will apply where Customer is a processor of Customer Data and Kajabi is processing Customer Data.

2. **For Transfers From the United Kingdom**

   2.1. Attachment 4: (UK Controller to Processor) The Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU will apply where Customer is a controller of Customer Data and Kajabi is processing Customer Data.

   2.2. Attachment 5: (UK Controller to Controller) The Standard Contractual Clauses for data controller to data controller transfers approved by the European Commission in decision 2004/915/EC will apply where Kajabi is processing Customer Account Data or Product Generated Data.

3. **Conflict.** To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA or the Agreement provisions of the Standard Contractual Clauses will prevail.