



## DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) is made by and between AlayaCare Inc. (“**AlayaCare**”) and the company or other legal entity (the “**Customer**”) who enters into the Master Subscription and Services Agreement (the “**Agreement**”) for the provision of the “**Services**” (as that term is defined in the Agreement). This DPA is effective as of the date AlayaCare and the Customer enter into the Agreement (the “**Effective Date**,” which shall be the same as the Effective Date of the Agreement).

AlayaCare and Customer shall hereafter be collectively known as the “**Parties**” and individually known as a “**Party**”. To the extent that any of the terms or conditions contained in this DPA may contradict or conflict with any terms or conditions regarding the processing of Personal Information in the Agreement, it is expressly understood and agreed that the terms of this DPA shall take precedence and supersede those other terms or conditions as it regards the subject matter.

The Parties agree as follows:

### 1. DEFINITIONS

1.1 For the purposes of this DPA, the following expressions bear the following meanings unless the context otherwise requires:

“**Applicable Data Protection Laws**” means, in respect of a Party, any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument relating to the protection of Personal Information, including:

(a) Canada’s “**PIPEDA**” (the *Personal Information Protection and Electronic Documents Act*);

(b) Ontario’s *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A (“**PHIPA**”);

(c) Quebec’s *Act Respecting the Protection of Personal Information in the Private Sector* as amended by Law 25 (the “**Quebec Privacy Act**”);

(d) the *Health Insurance Portability and Accountability Act* of 1996 (“**HIPAA**”) in the United States;

(e) the *California Consumer Privacy Act* (“**CCPA**”) as amended by the *California Privacy Rights Act*;

(e) any other state privacy laws in force in the United States, such as those which are currently in force in Colorado, Connecticut, and Virginia;

(f) Australia’s *Privacy Act 1988*; and

(g) New Zealand’s *Privacy Act 2020*;



(in each case as amended, consolidated, re-enacted or replaced from time to time).

**“Data Subject”** means an identified or identifiable natural person. Data Subject shall also mean “natural person” as defined in the Quebec Privacy Act;

**“Protected Health Information”** or **“PHI”** means any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. PHI shall also mean **“Personal Health Information”** as defined in section 4 of PHIPA.

**“Personal Information”** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject;

**“Processing”** (or any grammatical form thereof) means any operation or set of operations that are performed on Personal Information or on sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing shall also mean to “collect, hold, use or communicate to third parties” as found in the Quebec Privacy Act;

**“Regulator”** means the data protection supervisory authority which has jurisdiction over the Data Controller’s Processing of Personal Information. This includes but is not limited to the Information and Privacy Commissioner and the Assistant Commissioner for Personal Health Information in Ontario, the *Commission d’accès à l’information* in Quebec, and California’s Office of the Attorney General.

Any capitalized terms used but not defined herein shall have the meaning given to them in the Agreement.

## **2. PROCESSING OF PERSONAL INFORMATION**

- 2.1** The Parties acknowledge and agree that with regard to the Processing of Personal Information, Customer is the **“Data Controller”**, AlayaCare is the **“Data Processor”** and that AlayaCare will engage **“Sub-Processors”** pursuant to the requirements set forth in Section 8 below.
- 2.2** The duration of the Processing, the nature and purpose of the Processing, the types of Personal Information and categories of Data Subjects Processed under this DPA are further specified in **Schedule 1 “Processing Details”** of this DPA.
- 2.3** The Data Processor shall only Process the Personal Information on behalf of and in



accordance with documented instructions from the Data Controller. The Parties agree that this DPA (including all other agreements mentioned herein) is Customer's complete and final instructions to AlayaCare in relation to processing of Customer Data. The Data Controller shall ensure that its instructions comply with all Applicable Data Protection Laws, and that the Processing of Personal Information in accordance with Data Controller's instructions will not cause Data Processor to be in breach of the Applicable Data Protection Laws. The Data Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Information and the means by which the Data Controller acquired Personal Information and shall establish the legal basis for Processing under Applicable Data Protection Laws.

**2.4** Each Party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Applicable Data Protection Laws.

**2.5** The Data Controller shall have the right to verify the Processing of Personal Information by the Data Processor as required by the Applicable Data Protection Laws.

### **3. AUTHORIZED PERSONNEL**

**3.1** The Data Processor shall ensure that its personnel authorized to Process the Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Data Processor shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

### **4. RIGHTS OF DATA SUBJECTS**

**4.1** The Data Processor shall, to the extent legally permitted, promptly notify the Data Controller if it receives a request from a Data Subject for access to its own Personal Information, or for the rectification or erasure of such Personal Information or any other request or query from a Data Subject relating to its own Personal Information (including Data Subjects' exercising rights under Applicable Data Protection Laws, such as rights of objection, restriction of processing, data portability, right to be forgotten including de-indexation rights, or the right not to be subject to automated decision making) (a "**Data Subject Request**"). Taking into account the nature of the Processing, the Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to a Data Subject Request under Applicable Data Protection Laws. In addition, to the extent the Data Controller, in its use of the Services, does not have the ability to address a Data Subject Request, the Data Processor shall upon Data Controller's request provide commercially reasonable efforts to assist the Data Controller in responding to such Data Subject Request, to the extent the Data Processor is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws. To the extent legally permitted, the Data Controller shall be responsible for any costs arising from the Data Processor's provision of such assistance.

### **5. GOVERNMENT ACCESS REQUESTS**

**5.1** The Data Processor shall promptly notify the Data Controller about any legally binding



request for disclosure of Personal Information by a law enforcement authority, unless otherwise prohibited from doing so. The Data Controller shall have the right to defend such action in lieu of and/or on behalf of the Data Processor. The Data Processor shall reasonably cooperate with the Data Controller in such defense.

## 6. SECURITY

- 6.1 The Data Processor shall implement and maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Information), confidentiality and integrity of Personal Information.
- 6.2 The Data processor acknowledges and agrees that the Personal Information Processed under this DPA includes PHI (as specified in Appendix A), and has implemented heightened technical and organizational measures for the protection of the PHI as required by the Applicable Data Protection Laws.
- 6.3 Details regarding the technical and organizational measures as well as other measures for the protection of protection of Person Information can be found at <https://trustcenter.alayacare.com/>. Data Processor shall keep that information up to date on a regular basis.

## 7. COMPLIANCE

- 7.1 The Data Processor shall take reasonable efforts to make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and Applicable Data Protection Laws.
- 7.2 Upon Data Controller's request, the Data Processor shall provide the Data Controller with reasonable cooperation and assistance needed to fulfil Data Controller's obligations under Applicable Data Protection Laws to carry out a data protection impact assessment or privacy impact assessment related to Data Controller's use of the Services, to the extent the Data Controller does not otherwise have access to the relevant information, and to the extent such information is available to the Data Processor. The Data Processor shall provide reasonable assistance to the Data Controller in the cooperation or prior consultation with the Regulator in the performance of its tasks relating to Section 7 of this DPA, to the extent required under the Applicable Data Protection Laws.

## 8. SUB-PROCESSING

- 8.1 The Data Controller agrees that the Data Processor may engage Sub-Processors to Process Personal Information. The Sub-Processors currently engaged by AlayaCare and authorized by the Customer are listed in **Schedule 2 "List of Sub-Processors"**
- 8.2 The Data Processor shall ensure that each Sub-Processor has entered into a written agreement requiring the Sub-Processor to abide by terms no less protective than those provided in this DPA. The Data Processor shall be liable for the acts and omissions of any Sub-Processors to the same extent as if the acts or omissions were performed by

the Data Processor.

- 8.3** The Data Processor shall make available to the Data Controller a list of Sub-Processors authorized to Process Personal Information (“**Sub-Processor List**”, currently found in Schedule 2) and provide the Data Controller with a mechanism to obtain notice of any updates to the Sub-Processor List. Notification of a new Sub-Processor shall be issued prior to such new Sub-Processor being authorised to Process Personal Information in connection with the Agreement.
- 8.4** The Data Controller may object to Data Processor’s use of a new Sub-Processor where there are reasonable grounds to believe that the new Sub-Processor will be unable to comply with the terms of this DPA or the Agreement. If the Data Controller objects to Data Processor’s use of a new Sub-Processor, the Data Controller shall notify the Data Processor promptly in writing within ten (10) days after notification regarding such Sub-Processor. Data Controller’s failure to object in writing within such time period shall constitute approval to use the new Sub-Processor. The Data Controller acknowledges that the inability to use a particular new Sub-Processor may result in delay in providing the Services, inability to provide the Services or increased fees. The Data Processor will notify the Data Controller in writing (including by email) of any change to the Services or fees that would result from Data Processor’s inability to use a new Sub-Processor to which the Data Controller has objected. The Data Controller may either execute a written amendment to the Agreement implementing such change or exercise its right to terminate the Agreement in accordance with the termination provisions thereof. Such termination shall not constitute termination for breach of the Agreement. The Data Processor shall have a right to terminate the Agreement if the Data Controller unreasonably objects to a Sub-Processor, or does not agree to a written amendment to the Agreement implementing changes in fees or the Services resulting from the inability to use the Sub-Processor at issue.

## **9. RETURN AND DELETION**

- 9.1** The Data Processor shall, at the choice of the Data Controller, delete (and confirm such deletion in writing) or return all the Personal Information to the Data Controller after the end of the provision of the Services relating to Processing, and delete existing copies of the Personal Information unless prohibited by law or the order of a governmental or regulatory body or it could subject the Data Processor to liability. Data Processor may also anonymize such Personal Information and retain copies of anonymized Personal Information if permitted by the Applicable Data Protection Laws.
- 9.2** The Data Controller acknowledges and agrees that the Data Processor shall have no liability for any losses incurred by the Data Controller arising from or in connection with Data Processor’s inability to provide the Services as a result of Data Processor complying with a request to delete or return Personal Information made by the Data Controller pursuant to Section 9.1.

## **10. DATA BREACH**

- 10.1** In the event there is, or Data Processor reasonably believes that there is, any improper, unauthorized or unlawful access to, use of, or disclosure of, or any other compromise

which affects the availability, integrity or confidentiality of Personal Information which is Processed by Data Processor under or in connection with this DPA and/or the Agreement (a “**Data Breach**”), then upon becoming aware of such Data Breach, Data Processor shall promptly notify the Data Controller and provide the Data Controller with the following information as it becomes available:

(i) a description of the nature of the Data Breach, including where possible the categories and approximate number of Data Subjects concerned;

(ii) the name and contact details of the Data Processor contact from whom more information can be obtained; and

(iii) a description of the measures taken or proposed to be taken to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

**10.2** The Parties agree to coordinate in good faith on developing the content of any related public statements and any required notices to the affected Data Subjects and/or the relevant Regulators in connection with a Data Breach, provided that nothing in this Section 10.2 shall prevent either party from complying with its obligations under Applicable Data Protection Laws. The Parties further acknowledge and agree to use the established standards under Applicable Data Protection Laws to determine whether to notify the affected Data Subjects and/or the relevant Regulators, including but not limited to the “real risk of significant harm” under PIPEDA and the “risk of serious injury” of the Quebec Privacy Act.

## **11. GENERAL PROVISIONS**

**11.1 Term and Termination.** This DPA will terminate upon termination of the Agreement or when the Data Processor ceases to Process Personal Information, whichever is later, unless otherwise agreed in writing between the Parties.

**11.2 Remedies.** The Parties hereby acknowledge and agree that a person with rights under this DPA may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this DPA shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this DPA.

**11.3 Changes.** If one of the Parties seeks changes to the DPA to comply with a change in Applicable Data Protection Laws or binding and final decision of a Regulator with jurisdiction over the Party’ Processing of Personal Information, the Parties will discuss in good faith how to address any necessary changes.

**11.4 Other Similar Agreements and Addenda.** The Parties acknowledge and agree that in the event the Customer is in the United States, the Parties shall enter into a Business Associate Agreement (“**BAA**”) governing the processing of Protected Health Information (PHI) under HIPAA and the Health Information Technology for Economic and Clinical Health Act. In addition, Customers in the United States are governed by the AlayaCare



Privacy & Security Addendum available at <https://alayacare.com/wp-content/uploads/2024/01/privacy-security-addendum-to-MSSA-AC24.1-US.pdf>. In the event of a conflict between the documents related to the subject matter, the order of precedence to the extent necessary to resolve the conflict shall be: (1) the BAA; (2) this DPA; (3) the Privacy & Security Addendum.

**11.5 Headings.** The section and sub-section headings contained in this DPA are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPA.



## **SCHEDULE 1: PROCESSING DETAILS**

### **Processing Activities**

*The Personal Information Processed by Data Processor will be subject to the following basic Processing activities:*

Provision of the Services, as outlined in the Agreement and as otherwise agreed upon by the Parties.

### **Duration**

*The Personal Information Processed by Data Processor will be Processed for the following duration:*

The length of the term of the Agreement between Data Controller and Data Processor.

### **Data Subjects**

*The Personal Information Processed by Data Processor concern the following categories of Data Subjects:*

Customers and their Clients and Users, as those terms are defined and described in the Agreement.

### **Categories of Data**

*The Personal Information Processed by Data Processor includes the following categories of data:*

Customer information:

- Contact information (First name, Last name, Phone, Email, Gender)
- Address (includes civic address, city / town, postal code, country)
- Invoicing and billing information (credit card holder name, last 4 digits of the credit card number, expiration date, and billing address)

Client information:

- First name, Last name
- Email
- Phone
- Gender
- Additional information – any other Personal Information (as defined under applicable Data Protection laws) that the Customer collects from its users through the Services

Analytics information:

- Unique analytics identifiers



- IP addresses

Security information:

- IP addresses
- Country
- Email

Advertising information:

- Unique advertising identifiers

**Special Categories of Data (if applicable)**

*The Personal Information Processed by Data Processor concern the following special categories of data:*

Protected Health Information / Personal Health Information.



## SCHEDULE 2: LIST OF SUB-PROCESSORS

| Sub-Processor Name<br>(Sub-Processor activity)    | Location and Where to Find More Information   |
|---|---|
| <b>Hubspot</b><br>(Customer Relations Management) | United States, Cambridge, Massachusetts<br><a href="https://legal.hubspot.com/privacy-policy">https://legal.hubspot.com/privacy-policy</a>                    |
| <b>Amazon Web Services</b><br>(Cloud provider)    | USA, Canada, Australia<br><a href="https://aws.amazon.com/privacy/">https://aws.amazon.com/privacy/</a>   |
| <b>Google Looker</b><br>(Data analytics)          | USA, Canada, Australia<br><a href="https://cloud.google.com/looker/docs/studio/privacy-policy">https://cloud.google.com/looker/docs/studio/privacy-policy</a> |
| <b>Sendbird</b><br>(Collaboration)                | USA, Canada, Australia<br><a href="https://sendbird.com/dpf">https://sendbird.com/dpf</a>   |
| <b>Snowflake</b><br>(Data storage and processing) | USA, Canada, Australia<br><a href="https://www.snowflake.com/en/legal/privacy/privacy-policy/">https://www.snowflake.com/en/legal/privacy/privacy-policy/</a> |
| <b>OneSchema</b><br>(Data storage and processing) | USA, Canada, Australia<br><a href="https://www.oneschema.co/privacy-notice">https://www.oneschema.co/privacy-notice</a>                                       |
| <b>Box</b><br>(Data storage and processing)       | USA, Canada, Australia<br><a href="https://www.box.com/en-ca/legal/privacypolicy">https://www.box.com/en-ca/legal/privacypolicy</a>                           |