

Exhibit B
Data Processing Addendum

This Data Processing Addendum, including its appendices (the "**Addendum**"), supplements and forms part of the Agreement.

1. Definitions

For purposes of this Addendum, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this Addendum have the meanings given in the Agreement.

- 1.1 **Applicable Data Protection Laws** means the laws of any jurisdiction applicable to the confidentiality, privacy and/or security of Personal Information or processing thereof under the Agreement, including, without limitation, the CCPA.
- 1.2 **CCPA** means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time.
- 1.3 **Information Security Incident** means a breach of Activate's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information in Activate's possession, custody or control.
- 1.1 **Personal Information** means any information that Activate processes on behalf of Customer or any information Customer provides to Activate for the provision of the Activate Service that constitutes "personal information", "personally identifiable information", "personal data" or similar information governed by the CCPA or other Applicable Data Protection Laws, except that Personal Information does not include such information pertaining to Customer's personnel or representatives who are end users of the Activate Service or business contacts of Activate.
- 1.4 **Security Measures** has the meaning given in Section 4.1 (**Activate's Security Measures**).
- 1.5 **Subprocessors** means third parties engaged by Activate who are authorized under this Addendum to process Personal Information in relation to the Activate Service.

2. Duration and Scope of Addendum

- 2.1 This Addendum will, notwithstanding the expiration of the Agreement, remain in effect until, and automatically expire upon, Activate's deletion of all Personal Information.
- 2.2 Annex 1 (California Annex) to this Addendum, applies to Personal Information or the processing thereof subject to the CCPA.

3. Personal Information Processing

Activate will process Personal Information only in compliance with Applicable Data Protection Laws and only as necessary to perform its obligations and exercise its rights under the Agreement. For the purposes of this Addendum, Customer is the sole owner of Personal Information, and only Customer shall have the right to direct Activate in connection with Activate's processing of Personal Information.

4. Security

- 4.1 Activate Security Measures. Activate will implement and maintain reasonable technical and organizational measures designed to protect Personal Information against Information Security Incidents, including, without limitation, the measures described in Annex 2 (the "**Security Measures**"). Such Security Measures shall comply with Applicable Data Protection Laws.
- 4.2 Information Security Incidents. If Activate becomes aware of an Information Security Incident, Activate will (a) notify Customer of the Information Security Incident without undue delay and as quickly as reasonably possible after becoming aware of the Information Security Incident and (b) take reasonable steps to identify the cause of such Information Security Incident, minimize harm and prevent a recurrence. Notifications made pursuant to this Section 4.2 will describe, to the extent possible, details of the Information Security Incident, including steps taken to mitigate the potential risks, steps Activate recommends Customer take to address the Information Security Incident, the type of Personal Information that was subject to the Information Security Incident, and the identity of each affected person. Unless required to do so under Applicable Data Protection Laws, Activate shall not release or publish any filing, communication, notice, press release, or report concerning any Information Security Incident without Customer's prior written approval.

5. Data Subject Rights

- 5.1 Customer's Responsibility for Requests. If Activate receives any request from an individual in relation to the data subject's Personal Information, Activate will notify Customer in writing of such requests promptly, and Activate shall not take any action in response to such request except in accordance with Customer's written instructions.
- 5.2 Activate's Data Subject Request Assistance. Activate will (taking into account the nature of the processing of Personal Information) provide Customer with self-service functionality through the Activate Service or other reasonable assistance as necessary for Customer to perform its obligation under Applicable Data Protection Law to fulfill requests by individuals to exercise their rights under Applicable Data Protection Laws within any deadlines imposed thereunder. In the event the self-service functionality does not adequately allow Customer to respond to a data subject request, Activate shall implement and maintain reasonable and appropriate technical measures that will ensure that Customer's reasonable and lawful instructions can be complied with, including: (a) updating, amending, correcting, deleting, or providing access to the Personal Information of any data subject upon written request of Customer from time to time; and (b) facilitating Customer's responses to data subject requests as required under Applicable Data Protection Laws.

6. Audits

- 6.1 Customer may audit Activate's compliance with its obligations under this Addendum up to once per year, in the event of an Information Security Incident, and on such other occasions as may be required by Applicable Data Protection Laws. In the event that Customer desires to exercise its right to audit up to once per year, Customer shall provide Activate with no less than fourteen (14) days' notice prior to its intended audit date.
- 6.2 If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and Activate has certified in writing that there are no known material changes in the controls audited, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures, unless such audit is in response to an Information Security Incident or a requirement under Applicable Data Protection Laws.
- 6.3 The audit must be conducted during regular business hours, and may not unreasonably interfere with Activate's business activities.
- 6.4 Any audits are at Customer's expense unless the audit identifies noncompliance with this Addendum in any material respect, in which case Activate will reimburse Customer for all of its out of pocket costs and expenses associated with the audit.

7. Subprocessors

- 7.1 Consent to Subprocessor Engagement. Subject to this Addendum, Customer generally authorizes the engagement of Subprocessors.
- 7.2 Current Subprocessors. All Subprocessors engaged by Activate as of the date of this Addendum, if any, and a description of their functions are as follows:
- Amazon AWS, USA, Cloud Infrastructure for our apps and services
 - MongoDB, Inc., USA, Data storage
 - AWS S3, AWS Storage Solution
- 7.3 Engaging New Subprocessors. When engaging any Subprocessor, Activate will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this Addendum with respect to Personal Information. Activate shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor. Activate shall not permit any Subprocessor to process Personal Information in or from any location outside of the United States, Canada or the European Union without Customer's prior written consent.
- 7.4 Opportunity to Object to Subprocessor Changes. When any new Subprocessor not listed in Section 7.2 is engaged during the term of the Agreement, Activate will notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) at least 30 days prior to such engagement. If Customer objects to such engagement in a written notice to Activate within 30 days of being informed thereof on reasonable grounds relating to the protection of Personal Information, Customer and Activate will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Activate Service by providing written notice to Activate and receive a refund of any prepaid fees under the

Agreement.

8. Termination

Upon termination of Customer's access to the Activate Services, Activate shall, within fourteen (14) days of such termination, delete, destroy, or otherwise dispose of any and all Customer information and/or Personal Information in the care, custody or control of Activate and any Subprocessor, except to the extent retention thereof is required by law. In the event retention of Personal Information is required by law, Activate shall retain such information in accordance with this Addendum and Applicable Data Protection Laws. Customer shall further dispose of any and all signs or other materials which contain its QR Codes as issued to it by Activate.

9. Prohibited Data

Customer represents and warrants to Activate that Customer has not provided and will not provide, without Activate's prior written consent, the following for Customer to Process: any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; credit reports or consumer reports; any payment card information subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or the regulations promulgated under either such law; information subject to restrictions under Applicable Data Protection Laws governing Personal Information of children, including, without limitation, all information about children under 13 years of age.

10. Miscellaneous

Except as expressly modified by the Addendum, the terms of the Agreement remain in full force and effect. The requirements of this Addendum are in addition to and not in lieu of the requirements of the Agreement. To the extent of any conflict or inconsistency between this Addendum and the other terms of the Agreement, this Addendum will govern. In the event Activate's processing of Personal Information includes the processing of Personal Information of individuals in the European Economic Area, the United Kingdom, or another jurisdiction with comprehensive privacy laws, the Parties agree to comply with any and all laws of the other jurisdiction.