Exhibit B

Seventh Sense Data Processing Addendum

Last Updated: October 27, 2021

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the Master Services Agreement, Terms of Service or other written or electronic agreement between Telepath Data, Inc. dba Seventh Sense, Inc. ("**Vendor**") and the legal entity defined as 'Customer' thereunder together with all Customer Affiliates who are signatories to an Order Form for their own Account (as defined in Section 1 below) pursuant to such agreement (collectively, for purposes of this DPA, "**Customer**", and together with Vendor, the "**parties**") (such agreement, the "**Agreement**"). This DPA shall be effective on the effective date of the Agreement, unless this DPA is separately executed in which case it's effective on the date of the last signature ("**DPA Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions.

"**Account**" means Customer's account in the Service in which Customer stores and processes Customer Data.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Authorized Affiliate**" shall mean a Customer Affiliate who has not signed an Order Form pursuant to the Agreement, but is either a Data Controller or Data Processor for the Customer Personal Data processed by Vendor pursuant to the Agreement, for so long as such entity remains a Customer Affiliate.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended from time to time.

"**Customer Data**" has the meaning set forth in the Agreement.

"**Customer Personal Data**" means any Customer Data that is Personal Data.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU & UK Data Protection Law and the CCPA.

"**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

"**EU & UK Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); and (ii) the GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2018.

"**Personal Data**" means any information, including opinions, relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including, but not limited to, the definition of "personal information" in the CCPA.

"**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and "Process", "Processes" and "Processed" will be interpreted accordingly.

"**Purposes**" shall mean (i) Vendor's provision of the Services as described in the Agreement, including Processing initiated by End Users in their use of the Services; and (ii) further documented, reasonable instructions from Customer agreed upon by the parties.

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

"**Sensitive Data**" means (i) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (ii) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (iii) employment, financial, credit, genetic, biometric or health information; (iv) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (v) account passwords; or (vi) other information that falls within the definition of "special categories of data" or "special personal information" under applicable Data Protection Laws.

"**Services**" means the generally available Vendor software-as-a-service offering described in the Documentation and procured by Customer, and any other services provided by Vendor as described under the Agreement, including but not limited to support and technical services.

"**Vendor Group**" means Vendor Inc. and its Affiliates.

"**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries approved pursuant to Commission Decision (EU) 2021/914 of 4 June 2021, found at ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

"**Sub-Processor**" means any other Data Processors engaged by a member of the Vendor Group to Process Customer Personal Data.

2. Scope and Applicability of this DPA. This DPA applies where and only to the extent that Vendor Processes Customer Personal Data on behalf of Customer as Data Processor in the course of providing the Services.

3. Roles and Scope of Processing.

3.1. **Role of the Parties**. As between Vendor and Customer, Vendor shall Process Customer Personal Data only as a Data Processor (or sub-processor) acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein, in each case regardless of whether Customer acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller ("**Third-Party Controller**") with respect to Customer Personal Data. To the extent any Enhancement Data (as defined in the Agreement) is considered Personal Data under applicable Data Protection Laws, Vendor is the Data Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws.

3.2. **Customer Instructions**. Vendor will Process Customer Personal Data only for the Purposes. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out the exclusive and final instructions to Vendor for all Processing of Customer Personal Data, and (if applicable) include and are consistent with all instructions from Third-Party Controllers. Any additional requested instructions requires the prior written agreement of Vendor. Vendor shall promptly notify Customer if, in Vendor's opinion, such an instruction violates EU & UK Data Protection Law. Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with a Third-Party Controller.

3.3. **Customer Affiliates**. Vendor's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions:

(a) Customer must exclusively communicate any additional Processing instructions requested pursuant to 3.2 directly to Vendor, including instructions from its Authorized Affiliates;

(b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer; and

(c) Authorized Affiliates shall not bring a claim directly against Vendor. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Vendor ("**Authorized Affiliate Claim**"): (i) Customer must bring such Authorized Affiliate Claim directly against Vendor on behalf of such Authorized Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim; and (ii) all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

3.4. **Customer Processing of Personal Data**. Customer agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Customer Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing and backing-up Customer Personal Data; and (iii) has obtained all consents, permissions and rights necessary under Data Protection Laws for Vendor to lawfully Process Customer Personal Data for the Purposes, including, without limitation, Customer's sharing and/or receiving of Customer Personal Data with third parties via the Services.

3.5. **Details of Data Processing**.

(a) Subject Matter. The subject matter of the Processing under this DPA is the Customer Personal Data.

(b) Frequency and duration. Notwithstanding expiry or termination of the Agreement, Vendor will Process the Customer Personal Data continuously and until deletion of all Customer Personal Data as described in this DPA.

(c) Purpose. Vendor will Process the Customer Personal Data for the Purposes, as described in this DPA.

(d) Nature of the Processing. Vendor will perform Processing as needed for the Purposes, and to comply with Customer's Processing instructions as provided in accordance with the Agreement and this DPA.

(e) Retention Period. The period for which Customer Personal Data will be retained and the criteria used to determine that period shall be determined by Customer during the term of the Agreement via its use and configuration of the Services. Upon termination or expiration of the Agreement, Customer may retrieve or delete all Customer Personal Data as set forth in the Agreement. Any Customer Personal Data not deleted by Customer shall be deleted by Vendor promptly upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement.

(f) Categories of Data Subjects. The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);

(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors; and/or

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons).

(g) Categories of Personal Data. The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, title, contact details);

(ii) Employment details (employer, job title, geographic location, area of responsibility); and/or

(iii) IT information (IP addresses, cookies data, location data).

(h) Sensitive Data. Vendor does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Services.

4. Sub-Processing.

4.1. **Authorized Sub-Processors**. Customer provides Vendor with a general authorization to engage Sub-processors, subject to Section 4.3 (Changes to Sub-processors), as well as Vendor's current Sub-processors listed at https://theseventhsense.com/trust/sub-processors ("**Sub-processor Site**") as of the DPA Effective Date and members of the Vendor Group.

4.2. **Sub-Processor Obligations**. Vendor shall: (i) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as Vendor's obligations under this DPA to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA. Upon written request, and subject to any confidentiality restrictions, Vendor shall provide Customer all relevant information it reasonably can in connection with its applicable Sub-processor agreements where required to satisfy Customer's obligations under Data Protection Laws.

4.3. **Changes to Sub-Processors**. Vendor shall make available on its Sub-processor Site a mechanism to subscribe to notifications of new Sub-processors. Vendor shall provide such notification to those emails that have subscribed at least fourteen (14) days in advance of allowing the new Sub-processor to Process Customer Personal Data (the "**Objection Period**"). During the Objection Period, objections (if any) to Vendor's appointment of the new Sub-processor must be provided to Vendor in writing and based on reasonable grounds relating to data protection. In such event, the parties will discuss those objections in good faith with a view to achieving resolution. If it can be reasonably demonstrated to Vendor that the new Sub-processor is unable to Process Customer Personal Data in compliance with the terms of this DPA and Vendor cannot provide an alternative Sub-processor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may provide written notice to Vendor terminating the Order Form(s) with respect only to those aspects of the Services which cannot be provided by Vendor without the use of the new Sub-processor. Vendor will refund Customer any prepaid unused fees of such Order Form(s) following the effective date of termination with respect to such terminated Services.

5. Security.

5.1. **Security Measures**. Vendor shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data in accordance with Vendor's Information Security Overview found at https://www.theseventhsense.com/trust ("**Security Overview**"). Vendor may review and update its Security Overview from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

5.2. **Confidentiality of Processing**. Vendor shall ensure that any person who is authorized by Vendor to Process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3. **No Assessment of Customer Personal Data by Vendor**. Vendor shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for reviewing the information made available by Vendor relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

6. Customer Audit Rights.

6.1. Upon written request and at no additional cost to Customer, Vendor shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Vendor's compliance with its obligations under this DPA in the form of Vendor's most recently completed industry standard CAIQ security questionnaire (the "**Report**").

6.2. Customer may also send a written request for an audit of Vendor's applicable controls, including inspection of its facilities. Following receipt by Vendor of such request, Vendor and Customer shall mutually agree in advance on the details of the audit, including the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any such audit. Vendor may charge a fee (rates shall be reasonable, taking into account the resources expended by Vendor) for any such audit. The Report, audit, and any information arising therefrom shall be considered Vendor's Confidential Information and may only be shared with a third party (including a Third-Party Controller) with Vendor's prior written agreement.

6.3. Where the Auditor is a third party, the Auditor may be required to execute a separate confidentiality agreement with Vendor prior to any review of the Report or an audit of Vendor, and Vendor may object in writing to such Auditor, if in Vendor's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Vendor. Any such objection by Vendor will require Customer to either appoint another Auditor or conduct the audit itself. Any expenses incurred by an Auditor in connection with any review of the Report or an audit shall be borne exclusively by the Auditor. For clarity, the

exercise of audit rights under the SCCs shall be as described in this Section 6 (Customer Audit Rights) and Customer agrees these rights are carried out on behalf of Customer and all relevant Third-Party Controllers, subject to the confidentiality and non-use restrictions of the Agreement.

7. Data Transfers.

7.1. **Hosting and Processing Locations**. Vendor will only host Customer Personal Data in the region(s) offered by Vendor and selected by Customer on an Order Form or as Customer otherwise configures via the Services (the "**Hosting Region**"). Customer is solely responsible for the regions from which its End Users access the Customer Personal Data, for any transfer or sharing of Customer Personal Data by Customer or its End Users and for any subsequent designation of other Hosting Regions (either for the same Account, a different Account, or a separate Service). Once Customer has selected a Hosting Region, Vendor will not Process Customer Personal Data from outside the Hosting Region except as reasonably necessary to provide the Services procured by Customer, or as necessary to comply with the law or binding order of a governmental body.

7.2. **Transfer Mechanisms**. For any transfers by Customer of Customer Personal Data from the European Economic Area and its member states, United Kingdom and/or Switzerland (collectively, "**Restricted Countries**") to Vendor in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the applicable Data Protection Laws of the Restricted Countries) (collectively, "**Third Country**"), such transfers shall be governed by a valid mechanism for the lawful transfer of Customer Personal Data recognized under applicable Data Protection Laws, such as those directly below in 7.2.1. For clarity, for transfers from the United Kingdom and Switzerland, references in the SCCs shall be interpreted to include applicable terminology for those jurisdictions (e.g., 'Member State' shall be interpreted to mean 'United Kingdom' for transfers from the United Kingdom).

7.2.1. SCCs: Each party agrees to abide by and transfer Customer Personal Data from the Restricted Countries in accordance with the SCCs, which are incorporated into this DPA by reference. Each party is deemed to have executed the SCCs by entering into this DPA.

(a) The below shall apply to the SCCs, including the election of specific terms and/or optional clauses as described in more detail in (i)-(x) below, and any optional clauses not expressly selected are not included:

(i) The Module 2 terms apply to the extent Customer is a Data Controller and the Module 3 terms apply to the extent Customer is a Data Processor of the Customer Personal Data;

(ii) The optional Clause 7 in Section I of the SCCs is incorporated, and Authorized Affiliates may accede to this DPA and the SCCs under the same terms and conditions as Customer, subject to Section 3.3 of this DPA via mutual agreement of the parties;

(iii) For purposes of Clause 9 of the SCCs, Option 2 ('General written authorization') is selected and the process and time period for the addition or replacement of Sub-processors shall be as described in Section 4 (Sub-processing) of this DPA;

(iv) For purposes of Clause 13 and Annex 1.C of the SCCs, Customer shall maintain accurate records of the applicable Member State(s) and competent supervisory authority, which shall be made available to Vendor on request;

(v) For purposes of Clause 14(c), Customer may subscribe to the Sub-processor Site to receive notifications regarding updates to Vendor's overview of relevant laws and practices of Third Countries;

(vi) For purposes of Clause 17 and Clause 18 of the SCCs, the Member State for purposes of governing law and jurisdiction shall be the Netherlands;

(vii) For purposes of Annex 1.A, the 'data importer' shall be Vendor and the 'data exporter' shall be Customer and any Authorized Affiliates that have acceded to the SCCs pursuant to this DPA;

(viii) For purposes of Annex 1.B, the description of the transfer is as described in Section 3.5 (Details of Data Processing) of this DPA;

(ix) For purposes of Annex 2, the technical and organization measures are as follows: (i) Those measures implemented by Vendor shall be as described in Section 5.1 (Security Measures) of this DPA; and (ii) Those measures that can be

selected or configured by Customer, including appropriate controls for 'special categories of data', shall be as further described in Vendor's Documentation; and

(x) The Sub-processors for Annex III shall be as described in Section 4.1 (Authorized Sub-processors) of this DPA.

(b) Binding Corporate Rules for Processors ("**BCRs**"): Notwithstanding the foregoing, if Vendor has adopted BCRs for Processors that cover the transfer of Customer Personal Data to a Third Country, then such BCRs shall govern the transfer of Customer Personal Data.

8. Security Incident Response.

8.1. **Security Incident Reporting**. If Vendor becomes aware of a Security Incident, Vendor shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after becoming aware. Vendor's notification shall be sent to the email registered by Customer within the Service for such purposes, and where no such email is registered, Customer acknowledges that the means of notification shall be at Vendor's reasonable discretion and Vendor's ability to timely notify shall be negatively impacted. Vendor shall promptly take commercially reasonable steps to assist Customer in its efforts to contain, investigate, and mitigate any Security Incident.

8.2. **Security Incident Communications**. Vendor shall provide Customer timely information about the Security Incident, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Vendor to mitigate or contain the Security Incident, the status of Vendor's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Vendor personnel do not have visibility to the content of Customer Personal Data, it will be unlikely that Vendor can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, number or categories of affected Data Subjects. Communications by or on behalf of Vendor with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Vendor of any fault or liability with respect to the Security Incident.

9. **Cooperation.**

9.1. **Data Subject Requests**. Vendor shall promptly notify Customer if Vendor receives a request from a Data Subject that identifies Customer Personal Data or otherwise identifies Customer, including where the Data Subject seeks to exercise any of its rights under applicable Data Protection Laws (collectively, "**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to Data Subject Requests and Customer will be responsible for responding to any such Data Subject Requests. To the extent Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, Vendor shall (upon Customer's written request and taking into account the nature of the Processing) provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

9.2. **Data Protection Impact Assessments**. Vendor shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

9.3. **Government, Law Enforcement, and/or Third-Party Inquiries**. If Vendor receives a demand to retain, disclose, or otherwise Process Customer Personal Data for any third party, including, but not limited to law enforcement or a government authority ("**Third-Party Demand**"), then Vendor shall attempt to redirect the Third-Party Demand to Customer. Customer agrees that Vendor can provide information to such third-party as reasonably necessary to redirect the Third-Party Demand. If Vendor cannot redirect the Third-Party Demand to Customer, then Vendor shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy. This section does not diminish Vendor's obligations under the SCCs with respect to access by public authorities.

10. Relationship with the Agreement.

10.1. The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Vendor and Customer may have previously entered into in connection with the Services.

10.2. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing

of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Customer Personal Data comprised of patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state health care laws, rules or regulations ("**HIPAA Data**"), if there is any conflict between this DPA and a business associate agreement between Customer and Vendor ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data.

10.3. Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA, the SCCs, and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by one party (the "**Incurring Party**") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

10.4. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the SCCs).

10.5. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.