POWERSYNC DATA PROCESSING ADDENDUM

This Data Processing Agreement ("DPA") forms a part of the PowerSync Commercial License and Services Agreement, between Journey Mobile, Inc ("JourneyApps", "Supplier", "Service Provider" or "Processor") and _____ ("Customer" or "Controller") unless Customer has entered into a written Master Service Agreement with JourneyApps, in which case this DPA forms part of such written agreement, in either case, the "Agreement." This DPA is effective as of the date last signed below ("Effective Date").

1. DEFINITIONS

The following definitions and rules of interpretation apply to this DPA. Capitalised terms used in this DPA and not otherwise defined in the Agreement shall have the meaning given to them in the Data Protection Legislation.

1.1. **"Applicable Laws"** means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern a party.

1.2. **"Applicable Data Protection Laws"** means the Applicable Laws that govern how the Service may process or use an individual's Personal Data. For example, to the extent applicable, this includes: i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), ii) equivalent requirements in the Swiss Federal Data Protection Act and its Ordinance (Swiss DPA), iii) equivalent requirements in the United Kingdom including the Data Protection Act 2018, the United Kingdom General Data Protection Regulation ("UK Data Protection Law") and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and iv) US State Privacy Laws, in each case as may be amended from time to time.

1.3. **"CCPA"** means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and its implementing regulations.

1.4. **"Controller"** will have the meaning(s) given in the Applicable Data Protection Laws for the entity that determines the purpose and extent of Processing Personal Data.

1.5. **"Customer Personal Data"** means Personal Data that Customer uploads or provides to JourneyApps as part of the Service and that is governed by this DPA, as described under Annex I to this DPA.

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

1.7. **"Data Subject Request"** means a request from a Data Subject to access, correct, amend, transfer, or delete that Data Subject's Personal Data consistent with their rights under the Applicable Data Protection Laws.

1.8. **"European Economic Area"** or **"EEA"** means the member states of the European Union, Norway, Iceland, and Liechtenstein.

1.9. **"GDPR"** means European Union Regulation 2016/679 as implemented by local law in the relevant EEA member nation.

1.10. **"Personal Data"** will have the meaning(s) given in the Applicable Data Protection Laws for personal information, personal data, or other similar term.

1.11. **"Processing"** or **"Process"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12. **"Processor"** will have the meaning(s) given in the Applicable Data Protection Laws for the entity that Processes Personal Data on behalf of the Controller.

1.13. **"Security Incident"** means any confirmed unauthorized or unlawful breach of security that leads to the

accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data being Processed by JourneyApps. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

1.14. **"Sensitive Data"** means (a) racial or ethnic origin; (b) political opinions; (c) religious or philosophical beliefs; (d) trade union membership; (e) genetic data; (f) biometric data for the purpose of uniquely identifying a natural person; (g) data concerning health; (h) data concerning a natural person's sex life; (i) sexual orientation; and (ii) without limiting the foregoing, any additional information that falls within the definition of "special categories of data" under Applicable Data Protection Laws.

1.15. **"Service"** means the product and/or services provided by JourneyApps as specified in the Agreement executed by the parties.

1.16. **"Standard Contractual Clauses"** means, as applicable, (i) means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj; or (ii) the International Data Transfer Addendum to the EU Standard Contractual Clauses adopted by the UK Information Commissioner's Office effective March 21, 2022.

1.17. **"Subprocessor"** will have the meaning(s) given in the Applicable Data Protection Laws for an entity that, with the approval and acceptance of Controller, assists the Processor in Processing Personal Data on behalf of the Controller.

1.18. **"UK GDPR"** means European Union Regulation 2016/679 as implemented by section 3 of the United Kingdom's European Union (Withdrawal) Act of 2018 in the United Kingdom.

1.19. **"UK Addendum"** means the international data transfer addendum to the EEA SCCs issued by the Information Commissioner for Parties making Restricted Transfers under S119A(1) Data Protection Act 2018.

1.20. **"US State Privacy Laws"** means all US-state privacy laws and their implementing regulations, as amended or superseded from time to time, in effect, that apply to the Processing of Personal Data and that do not apply solely to specific industry sectors, demographics or specific classes of information.

2. ROLE, SCOPE AND DETAILS OF PROCESSING

2.1. **Relationship.** JourneyApps and Customer acknowledge and agree that for the purposes of the Applicable Data Protection Laws, (i) where Customer is the Controller of Customer Personal Data, JourneyApps will be deemed a Processor that is Processing Personal Data on behalf of Customer, and (ii) where Customer is a Processor of Customer Personal Data, JourneyApps will be deemed a Subprocessor.

2.2. **Details of Processing.** The subject-matter of Processing of Customer Personal Data by JourneyApps is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex I to this DPA.

2.3. **Compliance.** Each party will comply with its obligations under Applicable Data Protection Laws with respect to its Processing of Customer Personal Data.

2.4. **JourneyApps' Processing obligations.** To the extent that JourneyApps processes any Customer Personal Data on behalf of the Customer in connection with the Services, JourneyApps shall:

2.4.1. only Process such Customer Personal Data in accordance with the purposes set out in this Agreement and notify Customer immediately if in its opinion the Customer's instructions

infringe applicable law;

2.4.2. provide reasonable cooperation to Customer in connection with any data protection impact assessment (at Customer's expense only if such reasonable cooperation will require JourneyApps to assign significant resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Laws;

2.4.3. provide reasonable and timely assistance to Customer in complying with Customer's data protection obligations with respect to Data Subject Requests under Applicable Data Protection Laws. JourneyApps shall not respond to a Data Subject Request itself, except that Customer authorizes JourneyApps to redirect the Data Subject Request as necessary to allow Customer to respond directly;

2.4.4. ensure that access to any Customer Personal Data is restricted to those of its personnel who need to have access to perform the Services and who are subject to confidentiality obligations in respect of the Customer Personal Data; and

2.4.5. ensure that it has implemented appropriate technical and organizational measures, taking into account the nature of Processing and the information available to JourneyApps, including the measures set forth in Annex II of this DPA, without prejudice to JourneyApps' right to make future replacements or updates to the measures that do not lower the level of protection of Customer Personal Data.

2.5. **Customer's Processing obligations.** Customer shall ensure that:

2.5.1. its instructions comply with Applicable Data Protection Laws, and that JourneyApps' processing of Customer Personal Data, when done in accordance with Customer's instructions, will not cause JourneyApps to violate any Applicable Data Protection Laws.

2.5.2. that it has all necessary rights in relation to the Customer Personal Data and/or has collected all necessary consents from Data Subjects to Process Customer Personal Data to the extent required by Applicable Data Protection Laws.

3. SUBPROCESSORS

3.1. **Authorization.** Customer acknowledges and agrees that JourneyApps may engage subprocessors to Process Customer Personal Data on Customer's behalf in connection with the provision of Services. JourneyApps shall keep a list of its then-current Subprocessors (the "Subprocessor List") as set out at https://www.powersync.com/legal/subprocessors.

3.2. **Notification of Subprocessor changes.** The Subprocessor List may be updated from time-to-time as new Subprocessors are engaged by JourneyApps. Customer agrees that it is responsible for subscribing to the Customer Trust Portal in order to receive notifications of changes to the Subprocessor List. Updates to the Subprocessor List shall constitute notice to Customer of such changes via the Trust Center updates. If, within 10 calendar days of JourneyApps updating the Subprocessor List with a new Subprocessor, Customer notifies JourneyApps in writing of any objections (on reasonable grounds relating to data protection) to the new proposed appointment, Customer and JourneyApps will cooperate in good faith to resolve Customer's objection or concern. Customer acknowledges that certain Subprocessors are essential to providing the Services and that objecting to the use of a Subprocessor may prevent JourneyApps from continuing to offer the Services to Customer. Customer is deemed to consent to the updated Subprocessor List if Customer does not timely object within 10 calendar days of JourneyApps updating the Subprocessor List.

3.3. **Liability.** JourneyApps agrees to impose contractual data protection obligations on any Subprocessor it appoints that require such Subprocessor to protect Customer Personal Data as required by Applicable Data Protection Laws. JourneyApps will remain liable for any breach of this DPA that is caused by an act, error,

or omission of its Subprocessors.

4. SECURITY INCIDENTS

4.1. Upon becoming aware of a Security Incident, JourneyApps will notify Customer without undue delay, and in no event later than seventy-two (72) hours after JourneyApps' discovery of a Security Incident impacting Customer Personal Data, unless prohibited by Applicable Law.

4.2. Such notice will describe, to the extent possible, details of the Security Incident based on JourneyApps' then-current assessment, including steps taken to mitigate the potential risks and where applicable, steps JourneyApps recommends Customer take to address the Security Incident.

4.3. Without prejudice to JourneyApps' obligations under this section, Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Security Incidents. JourneyApps' notification of or response to a Security Incident will not be construed as an acknowledgement by JourneyApps of any fault or liability with respect to the Security Incident.

5. CROSS-BORDER DATA TRANSFERS

5.1. **Authorization.** Customer acknowledges and agrees that in order for JourneyApps to provide customers with service level continuity and to optimize both organization and management of the quality of its Service, JourneyApps reserves the right to have Customer Personal Data transferred and processed to a location where JourneyApps' Subprocessors maintain data processing operations, as indicated on the Subprocessor List. Such transfers shall be performed in accordance with the applicable requirements for cross-border transfers of Customer Personal Data under the Applicable Data Protection Laws.

5.2. **EEA Data transfers.** To the extent that JourneyApps is a recipient of Customer Personal Data protected by GDPR in a country outside of EEA that is not recognized as providing an adequate level of protection (as described in Applicable Data Protection Laws), the parties agree to abide by and process such Customer Personal Data in compliance with the Standard Contractual Clauses, which shall be incorporated into and form an integral part of this DPA as follows:

5.2.1. the Module Two (Controller to Processor) terms apply to the extent the Customer is a Controller of Customer Personal Data and the Module Three (Processor to Sub-processor) terms apply to the extent the Customer is a Processor of Customer Personal Data;

5.2.2. in Clause 7, the optional docking clause does not apply;

5.2.3. in Clause 9, Option 2 (general written authorization) applies and changes to Sub-Processors will be notified in accordance with section 3.2 of this DPA;

5.2.4. in Clause 11, the optional language does not apply;

5.2.5. All square brackets in Clause 13 are removed;

5.2.6. in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be the laws and courts of Ireland;

5.2.7. the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in the Annexes of this DPA; and

5.2.8. the supervisory authority that will act as competent supervisory authority will be the Irish Data Protection Authority.

5.3. **UK Data Transfers.** With respect to transfers to which the UK Data Protection Laws apply, the SCCs shall apply and shall be deemed amended as specified by the UK Addendum. The UK Addendum shall be

deemed executed by the parties and incorporated into and form an integral part of this DPA as follows:

5.3.1. The "exporter" is the Customer, and the exporter's contact information is set forth in Annex I(A) below;

5.3.2. The "importer" is JourneyApps and JourneyApps' contact information is set forth in Annex I(A) below;

5.3.3. The UK Information Commissioner is the exclusive Supervisory Authority for the transfers of UK Personal Data under this Agreement;

5.3.4. Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annexes of the relevant SCCs; and

5.3.5. Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

5.4. **Swiss Data Transfers.** With respect to transfers to which the Swiss DPA apply, the SCCs shall apply in accordance with Section 5.2 with the following modifications:

5.4.1. References to "Member State" in the 2021 Standard Contractual Clauses refer to Switzerland, and data subjects may exercise and enforce their rights under the 2021 Standard Contractual Clauses in Switzerland;

5.4.2. References to GDPR in the 2021 Standard Contractual Clauses refer to the Swiss Federal Act on Data Protection (as amended and replaced);

5.4.3. Under Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commission to the extent that the transfer is governed by the Swiss Federal Act on Data Protection;

5.4.4. Clause 17 shall be replaced to state "The Clauses are governed by the laws of Switzerland"; and

5.4.5. Clause 18 shall be replaced to state "Any dispute arising from these Clauses shall be resolved by the applicable courts of Switzerland. The parties agree to submit themselves to the jurisdiction of such courts".

6. PROCESSING SUBJECT TO U.S STATE PRIVACY LAWS

6.1. This Section 6 applies to the extent that the Processing is subject to the Applicable Data Protection Laws of the U.S. states that have enacted Consumer Privacy Bills ("U.S. State Privacy Laws"). To the extent that JourneyApps' Processing of Customer Personal Data falls within the scope of the U.S. State Privacy Laws, the parties agree that (i) Customer is considered a "Business" under the U.S. State Privacy Laws and (ii) JourneyApps is acting as a "Service Provider," as such terms are defined pursuant to the U.S. State Privacy Laws.

6.2. JourneyApps will:

6.2.1. Process Customer Personal Data solely for the purpose of performing JourneyApps' obligations under the Agreement, including this DPA, and for no commercial purpose other than the performance of such obligations and improvement of the Service;

6.2.2. not retain, use or disclose the Customer Personal Data outside of the direct business relationship between Customer and JourneyApps;

6.2.3. not "sell" or "share" any Customer Personal Data, as such terms are defined in applicable U.S. State Privacy Laws, to any third party;

6.2.4. not attempt to re-identify any pseudonymized, anonymized, aggregate or de-identified Customer Personal Data without Customer's express written permission;

6.2.5. not combine Customer Personal Data with other Personal Data received or collected from or on behalf of other legal or natural persons for a purpose outside of the "business purpose" as that term is defined in the US State Privacy Laws;

6.2.6. provide the same level of protection for the Customer Personal Data as is required under the U.S. State Privacy Laws applicable to Customer;

6.2.7. not otherwise engage in any Processing of the Customer Personal Data that is prohibited or not permitted by "processors" or "service providers" under U.S. State Privacy Laws; and

6.2.8. promptly notify Customer if JourneyApps determines that it (i) can no longer meet its obligations under this DPA or U.S. State Privacy Laws; or (ii) has breached this DPA, and shall cooperate to remediate such breach.

7. AUDITS AND COMPLIANCE VERIFICATION

7.1. **Audit rights.** JourneyApps shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA with respect to Customer Personal Data ("Audit"). Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 7.1 and where applicable, the SCCs) and any audit rights granted by Applicable Data Protection Laws, by instructing JourneyApps to comply with the audit measures described in Sections 7.2 and 7.3 below.

7.2. **Security reports.** Customer acknowledges that JourneyApps is regularly audited against industry leading standards by independent third-party auditors. Upon written request, JourneyApps shall supply (on a confidential basis) a copy of its most current audit report(s) ("Report") to Customer, so that Customer can verify JourneyApps' compliance with the audit standards against which it has been assessed.

7.3. **Security due-diligence.** To the extent that JourneyApps' provision of a Report does not provide sufficient information for Customer to verify JourneyApps' compliance with this DPA or Customer is required to respond to a regulatory authority audit, JourneyApps will respond to reasonable requests for information made by Customer to confirm JourneyApps' compliance with this DPA, including responses to security and audit questionnaires, or by providing additional information about its information security and privacy program. However, JourneyApps may restrict access to data or information if Customer's access to the information would negatively impact JourneyApps' intellectual property rights, confidentiality obligations, or other obligations under Applicable Laws. All such requests must be in writing and may only be made once a year.

8. RETURN AND DELETION.

8.1. Upon termination or expiry of the Agreement, JourneyApps shall, at the instruction of Customer, return or delete all such Customer Personal Data in accordance with its requirements under Applicable Data Protection Laws, unless further storage is required or authorized by Applicable Law. In such a case, JourneyApps agrees to preserve the confidentiality of the Customer Personal Data retained by it and it will only Process such Customer Personal Data in order to comply with Applicable Law. Notwithstanding the foregoing, this provision will not require JourneyApps to delete Customer Personal Data from archival and back-up files except as provided by JourneyApps' internal data deletion practices or as required by Applicable Law.

8.2. If Customer and JourneyApps have entered the EEA SCCs or the UK Addendum as part of this DPA, JourneyApps will only give Customer the certification of deletion of Personal Data described in Clause 8.1(d) and Clause 8.5 of the EEA SCCs if Customer asks for one.

9. MISCELLANEOUS

9.1. **Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (i) the applicable terms in the Standard Contractual Clauses, (ii) the terms of this DPA; and (iii) the Agreement.

9.2. **Term of Agreement.** This DPA will start when JourneyApps and Customer sign or electronically accept this DPA or Agreement and will continue until the Agreement expires or is terminated. However, JourneyApps and Customer will each remain subject to the obligations in this DPA and Applicable Data Protection Laws until Customer stops transferring Customer Personal Data to JourneyApps and JourneyApps stops Processing Customer Personal Data on behalf of Customer.

9.3. **Liability Caps and Damages Waiver:** To the maximum extent permitted under Applicable Data Protection Laws, each party's total cumulative liability to the other party arising out of or related to this DPA will be subject to the waivers, exclusions, and limitations of liability stated in the Agreement.

9.4. **Related-Party Claims.** Any claims made against Provider or its Affiliates arising out of or related to this DPA may only be brought by the Customer entity that is a party to the Agreement.

9.5. **Exceptions.** This DPA does not limit any liability to an individual about the individual's data protection rights under Applicable Data Protection Laws. In addition, this DPA does not limit any liability between the parties for violations of the EEA SCCs or UK Addendum.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the last signature date below.

CUSTOMER	**JOURNEYAPPS**
By:	**By:**
Printed Name:	**Printed Name:**
Position/Title:	**Position/Title:**
Date:	**Date:**

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Customer, as specified in the Agreement

Contact details: as specified in the Agreement

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement.

Role: Controller.

Data importer(s):

Name: Journey Mobile, Inc

Contact details: JourneyApps' Data Protection Officer – dpo@journeyapps.com

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement.

Role: Processor.

B. DESCRIPTION OF DATA PROCESSING

Categories of Data Subjects:

- Customer's employees that use the JourneyApps platform
- Customer's end users/clients

Categories of Personal Data transferred: Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in their sole discretion, and which may include but is not limited to the following categories of Personal Data:

- Contact information (e.g., name, email address, and other account related information)
- System metadata (e.g., timestamps, identity of the device to access Services, location)
- Any other Personal Data submitted by, sent to, or received by Customer or their end users/clients via the Service such as phone numbers, Session Initiation Protocol Uniform Resource Identifier (SIP URI), call transcripts, call recordings, call logs, conversation messages and artifacts

Sensitive Data transferred: JourneyApps does not intentionally collect or Process any Sensitive Data in the provision of the Services. However, Customer may choose to transfer Sensitive Data, the extent of which is determined and controlled by Customer in their sole discretion. If Customer intends to process, transmit, or store protected health information (PHI) or payment card information (PCI) data, Customer must enable the appropriate compliance plan settings within the Services to designate their AI assistant as HIPAA- and/or PCI-compliant. When such settings (i.e., HIPAA or PCI mode) are enabled, no call logs, recordings, or transcriptions are stored and users are restricted to HIPAA/PCI compliant providers only.

Frequency of the transfer: Continuous basis depending on Customer's use of the Services.

Nature and purpose of the processing: JourneyApps offers a comprehensive high-performance data synchronization service.

As such, JourneyApps may Process Customer Personal Data as necessary to perform the Services pursuant to

the Agreement, including but not limited to Processing activities such as:

- Synchronization and replication of data between Customer's source databases and edge devices;
- Hosting and management of the PowerSync Service infrastructure;
- Transient caching and logging of data packets to ensure consistency and conflict resolution across distributed devices;
- Processing activities necessary for ongoing support, performance monitoring, and debugging of sync protocols;
- Processing necessary to maintain, optimize, and improve the synchronization engine provided to Customer; and
- Disclosure to third-parties in accordance with the Agreement, this DPA, or as compelled by applicable laws, which may include transfer of Personal Data to sub-processors (such as cloud infrastructure providers) on Customer's behalf and at their direction.

Duration of the processing: JourneyApps will Process Customer Personal Data for the duration of the Agreement.

C. SUB-PROCESSORS: as set out at https://www.powersync.com/legal/subprocessors.

D. COMPETENT SUPERVISORY AUTHORITY: as set out in Section 5 of this DPA.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

As of the effective date of this DPA, JourneyApps, when Processing Personal Data on behalf of the Customer implemented and maintains the following technical and organizational security measures for the Processing of such Personal Data:

1. **Information Security Program:** JourneyApps maintains and enforces a security program that addresses how JourneyApps manages security, including its security controls. The security program includes: (i) documented policies that JourneyApps formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually; (ii) documented, clear assignment of responsibility and authority for security program activities; and (iii) regular testing of the key controls, systems and procedures.
2. **Security Certifications:** JourneyApps selects an independent, qualified third-party auditor to conduct, at JourneyApps' expense, at least annual audit of the security of the Services and environments, in accordance with SOC 2, Type II standards or its equivalent.
3. **Access Controls:** JourneyApps takes reasonable measures to prevent Personal Data from being used without authorization. These controls vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factors authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.
4. **Transmission Controls:** JourneyApps takes reasonable measures to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport. Personal Data is encrypted in transit over public networks when communicating with JourneyApps user interfaces (UIs) and application programming interface (APIs) via industry standard HTTPS/TLS (TLS 1.2 or higher). Personal Data is encrypted at rest by JourneyApps´s Subprocessor and managed services provider, Amazon Web Services Inc., via AES-256.
5. **Logical separation controls:** JourneyApps implements measures to ensure that Personal Data collected for different purposes can be Processed separately, including segregation of functions (production/testing) and logical segmentation processes to manage the separation of Personal Data. Data from different JourneyApps' Customer environments is logically segregated on systems managed by JourneyApps to ensure that Customer Personal Data is segregated from one another.
6. **Human Resources Security:** All JourneyApps employees must sign non-disclosure agreements before gaining access to Personal Data. Every new employee must attend an information security training session during onboarding. After initial training, continuous training is provided which covers JourneyApps´s security policies, and security best practices on an annual basis, at a minimum.
7. **Vendor Management:** JourneyApps maintains a vendor management program to ensure that all Subprocessors undergo strict security and privacy due diligence, and data sharing is governed by signed agreements that include confidentiality, data protection, and access controls.
8. **Vulnerability Assessments.** JourneyApps performs periodic vulnerability assessments and annual independent third-party penetration testing on its systems and applications. Vulnerabilities that are detected are prioritized, categorized, and resolved promptly. Executive summaries of penetration test reports are available upon written request.
9. **Availability:** JourneyApps implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including database replication, backup procedures and a disaster recovery plan.
10. **Data Center Security:** JourneyApps uses reputable third-party service providers to host its production infrastructure and relies on these third-parties to manage the physical and environmental security controls to the data center facilities as part of JourneyApps' shared responsibility model.