DATA PROCESSING ADDENDUM

(Revision April 2024)

This Data Processing Addendum ("**DPA**") forms part of the PassKit Terms of Subscription Service Agreement or other written or electronic agreement between PassKit, Inc. and Customer (the "**Agreement**") for the purchase of online services from PassKit (identified either as "**Services**" or otherwise in the applicable agreement, and hereinafter defined as **"Services"** or **"PassKit Services**") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent PassKit processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the PassKit Services to Customer pursuant to the Agreement, PassKit will Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules. This DPA supersedes all prior and contemporaneous data processing agreements or data processing terms in any agreements, proposals or representations, written or oral, concerning the Processing of Personal Data.

DATA PROCESSING TERMS

1. DEFINITIONS

"Authorized Affiliate" means any of Customer's Affiliate(s) which (i) is subject to the data protection laws and regulations of the European Union, or the United Kingdom, and (ii) is permitted to use the PassKit Services pursuant to the Agreement between Customer and PassKit but has not completed the Registration process with PassKit and is not a "Customer" as defined under the Agreement.

"CCPA" means the California Consumer Privacy Act 2018, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations, as the same may be amended from time to time.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means what is defined in the Agreement as "Customer Data."

"Data Protection Laws and Regulations" means all laws and regulations applicable to a party in its use or provision of the PassKit Services, in connection with the Processing of Personal Data under the Agreement.

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

"Data Subject Right" means any right afforded to a Data Subject under Data Protection Laws and Regulations, including the rights to access, rectify, restrict the Processing of Personal Data, erasure (including the right to be forgotten), data portability, objecting to the Processing, or to not be subject to an automated individual decision making.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to an identified or identifiable natural person where such data is Customer Data.

"Processing" 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.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Personal Data Breach" means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by PassKit or its Sub-processors of which PassKit becomes aware.

"Security, Privacy and Architecture Datasheet" means the Security, Privacy and Architecture Datasheet for the PassKit Services, as updated from time to time.

"**UK Addendum**" means the International Data Transfer Addendum to the 2021 EU SCCs, issued by the Information Commissioner under S119A(1) Data Protection Act 2018, Version B1.0, that Customer and PassKit, Inc. may enter into, and that PassKit makes available at https://passkit.com/legal/.

"**2021 EU Standard Contractual Clauses**" or "**2021 EU SCCs**" means the "Controller to Processor" modules of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, that Customer and PassKit, Inc. may enter into and that PassKit makes available at https://passkit.com/legal/.

"2021 EU SCCs P2P" means the "Processor to Processor" modules of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 that PassKit may enter into with its Sub- processors.

"Sub-processor" means any Processor engaged by PassKit or its Affiliates engaged in the Processing of Personal Data.

2. PROCESSING OF PERSONAL DATA

2.1. **Details of the Processing.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, PassKit is the Processor and that PassKit or its Affiliates engaged in the Processing of Personal Data will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below. The subject matter of Processing of Personal Data by PassKit is the performance of the PassKit 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 Schedule 1 (Details of the Processing) to this DPA.

2.2. **Customer's Processing of Personal Data.** Customer shall, in its use of the PassKit Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. This DPA and the Agreement are, at the time of signature of the Agreement, Customer's complete and final documented instructions to PassKit for the Processing of Personal Data, and Customer's configuration of the PassKit Services shall constitute an additional instruction to PassKit. Any additional or alternate instructions must be agreed upon separately. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired the Personal Data.

2.3. **PassKit's Processing of Personal Data.** PassKit shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of Customer and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by

Users in their use of the PassKit Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. PassKit will Process Personal Data in compliance with applicable Data Protection Laws and Regulations, provided however that PassKit shall not be in violation of this contractual obligation in the event that PassKit's Processing of Personal Data in non-compliance with applicable Data Protection Laws and Regulations is due to Customer.

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Requests.** PassKit shall, to the extent legally permitted and to the extent PassKit has been able to identify that the request comes from a Data Subject whose Personal Data was submitted to the PassKit Services by Customer, promptly notify Customer if PassKit receives a request from a Data Subject in relation to the exercise of any Data Subject Right ("**Data Subject Request**"). PassKit will confirm to the Data Subject that it has passed the request to the Customer, but PassKit shall not handle or execute the Data Subject Request.

3.2. Taking into account the nature of the Processing, PassKit shall assist Customer by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

4. PASSKIT PERSONNEL

4.1. **Confidentiality.** PassKit shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. PassKit shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. **Reliability.** PassKit shall take commercially reasonable steps to ensure the reliability of any PassKit personnel engaged in the Processing of Personal Data.

4.3. **Limitation of Access.** PassKit shall ensure that PassKit's access to Personal Data is limited to those personnel performing PassKit Services in accordance with the Agreement.

4.4. **Data Protection Officer.** PassKit has appointed a data protection officer for PassKit and its Affiliates. The appointed person may be reached at privacy@passkit.com.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) PassKit's Affiliates may be retained as Sub- processors; and (b) PassKit and PassKit's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the PassKit Services. PassKit or a PassKit Affiliate has entered into a written agreement with each Sub-processor containing, in substance, the same data protection obligations as in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processor.

5.2. **List of Current Sub-processors and Notification of New Sub-processors.** Attached hereto as Schedule 3 is a current list of Sub-processors for the PassKit Services. Such Sub-processor list shall include the identities of those Sub-processors, their country of location as well as a description of the processing they perform. PassKit will notify Customer of a new Sub- processor(s) at least thirty (30) calendar days before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable PassKit Services. The notification shall include an updated Sub-processor list which is the information necessary to enable the Customer to exercise its right to object.

5.3. **Objection Right for New Sub-processors.** Customer may object to PassKit's use of a new Sub-processor by notifying PassKit promptly in writing within ten (10) calendar days after receipt of PassKit's notice in accordance with Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, PassKit will use reasonable efforts to make available to Customer a change in the PassKit Services or recommend a commercially reasonable change to Customer's configuration or use of the PassKit Services to avoid Processing of Personal Data by the objected-to new Sub- processor without unreasonably burdening Customer. If PassKit is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those PassKit Services which cannot be provided by PassKit without the use of the objected-to new Sub-processor, by providing written notice to PassKit. PassKit will refund to Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated PassKit Services, without imposing a penalty for such termination on Customer.

5.4. **Liability for Sub-processors.** PassKit shall be liable for the acts and omissions of its Sub-processors to the same extent PassKit would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1. **Controls for the Protection of Customer Data.** PassKit shall maintain appropriate technical and organizational measures for protection of the security (including protection against Personal Data Breach), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Datasheet attached hereto as Schedule 2. PassKit regularly monitors compliance with these measures. Customer is responsible for reviewing the information made available by PassKit relating to data security and making an independent determination as to whether the PassKit Services meet Customer's requirements and legal obligations under Data Protection Laws and Regulations. Customer acknowledges that the security measures described within the Security, Privacy and Architecture Datasheet are subject to technical progress and development and that PassKit may update or modify such document from time to time provided that such updates and modifications do not result in a material decrease of the overall security of the PassKit Services during a Subscription Term.

6.2. **Personal Data Incident Management and Notification.** PassKit maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Datasheet and shall notify Customer without undue delay after becoming aware of a Personal Data Breach. PassKit shall provide information to Customer necessary to enable Customer to comply with its obligations under Data Protection Laws and Regulations in relation to such Personal Data Breach. The content of such communication to Customer will (i) include the nature of Processing and the information available to PassKit, and (ii) take into account that under applicable Data Protection Laws and Regulations, Customer may need to notify regulators or individuals of the following: (a) a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of Personal Data records concerned; (b) a description of the likely consequences of the Personal Data Breach; and (c) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. PassKit shall make commercially reasonable efforts to identify the cause of such Personal Data Breach and take those steps as PassKit deems necessary and reasonable in order to remediate the cause of such Personal Data Breach to the extent the remediation is within PassKit's reasonable control. The obligation to remediate the cause of a Personal Data Breach shall not apply to Personal Data Breaches that are caused by Customer or Customer's Users.

6.3. **Third-Party Certifications and Audits.** PassKit has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Datasheet. Upon Customer's

written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, PassKit shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of PassKit and that is subject to confidentiality obligations substantially similar to those set forth in the Agreement) a copy of PassKit's then most recent third-party audits or certifications, as applicable, that PassKit makes available to its customers generally.

7. RETURN AND DELETION OF CUSTOMER DATA

The PassKit Services allow export and deletion of Customer Data during the Subscription Term. At the termination or expiration of the Agreement, PassKit shall return Customer Data by enabling Customer to export its Customer Data as set forth in the Agreement and shall delete Customer Data, in accordance with this DPA, the Agreement, applicable Data Protection Laws and Regulations and the Documentation. Upon request from the Customer, PassKit will provide a certificate of deletion once Customer Data has been deleted from the PassKit Services.

8. AFFILIATES

8.1. **Relationship between PassKit and Customer's Authorized Affiliates.** The parties acknowledge and agree that, by executing the Agreement, the Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing an independent DPA between PassKit and each such Authorized Affiliate, subject to the provisions of the Agreement and this Section 8 and Section 9. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For sake of clarity, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to this DPA. All access to and use of the PassKit Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

8.2. **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with PassKit under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates and Authorized Affiliates.

8.3. **Data Controller Rights of Affiliates and Authorized Affiliates.** Any Affiliate or Authorized Affiliate shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

Except where applicable Data Protection Laws and Regulations require the Affiliate or Authorized Affiliate to exercise a right or seek any remedy under this DPA against PassKit directly by itself, the parties agree that:

(i) solely the Customer that is the contracting party to the Agreement shall exercise any such right (including any Audit right) or seek any such remedy on behalf of such Affiliate or Authorized Affiliate,

(ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Affiliate or Authorized Affiliate individually but in a combined manner for all of its Affiliates and Authorized Affiliates together, and

(iii) when carrying out an on-site Audit, Customer shall take all reasonable measures to limit any impact on PassKit and its Sub-Processors by combining, to the extent reasonably possible, several Audit requests carried out on behalf of different Affiliates and Authorized Affiliates in one single Audit.

For the purpose of this Section 8.3, an Affiliate signing an Order Form with PassKit is not deemed "Customer".

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and PassKit, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

10. UK AND EU SPECIFIC PROVISIONS

The following provisions apply solely where Customer or an Authorized Affiliate is subject to the Data Protection Laws and Regulations of the United Kingdom or the European Union.

10.1. Data Protection Impact Assessment. Upon Customer's request, PassKit shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under applicable Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the PassKit Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to PassKit. PassKit shall provide reasonable assistance

to Customer in the cooperation or prior consultation with the Supervisory Authority (as defined in applicable Data Protection Laws and Regulations) in the performance of its tasks relating to this Section 10.1 of this DPA, to the extent required under applicable Data Protection Laws and Regulations.

10.2. **Infringing instructions.** PassKit shall immediately inform the Customer if, in its opinion, an instruction infringes applicable Data Protection Laws and Regulations.

10.3. **Audit right.** PassKit shall allow for and contribute to audits and inspections ("**Audits**"), not more than once per year. PassKit's contribution shall consist of PassKit's reasonable cooperation and making relevant PassKit employees available to Customer.

Such Audit may be conducted by Customer or Customer's independent, third-party auditor that is not a competitor of PassKit and that is subject to confidentiality obligations substantially similar to those set forth in the Agreement, at Customer's own cost:

(i) by PassKit providing information regarding PassKit's processing activities in the form of a copy of PassKit's then most recent third-party audit or certification, as applicable, that PassKit makes available to its customers generally and through its Documentation available at docs.passkit.io ;

(ii) to the extent required by applicable law, by PassKit allowing Customer to perform an On-Site Audit. "**On-site Audits**" shall be performed as follows: (a) an Audit of facilities operated by PassKit, carried out during normal business hours, (b) such Audit shall not exceed one (1) business day; (c) Customer will provide PassKit with at least three-weeks' written notice prior to such Audit, (d) before the commencement of any such Audit, Customer and PassKit shall mutually agree upon the scope, cost and timing of the Audit; (e) Customer shall promptly notify PassKit with information regarding any non-compliance discovered during the course of an Audit; and (f) Customer may perform an On-site Audit up to once per year.

10.4. **Transfer Mechanism(s) for Data Transfers.** As of the Effective Date of this DPA, with regard to any transfers of Personal Data under this DPA from the European Union, or the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations, PassKit makes available the following transfer mechanism(s) which shall apply, in the order of precedence as set out below, if applicable:

10.4.1. Any valid transfer mechanism pursuant to applicable EU and/or UK Data Protection Laws and Regulations (excluding the 2021 EU SCCs and the UK Addendum), to which PassKit would subscribe, certify or participate in.

10.4.2. Standard contractual clauses, being either the 2021 EU SCCs and/or the UK Addendum, when they are an available and a valid transfer mechanism under applicable Data Protection Laws and Regulations, and the parties acknowledge and agree that they will comply with such standard contractual clauses as set out below:

a) When and as applicable, Customer and any applicable Authorized Affiliates are each the data exporter, then Customer's signing of this DPA or an Agreement referencing this DPA, or a Customer's Affiliate signing an Order Form under an Agreement referencing this DPA, shall be treated as signing of the 2021 EU SCCs and their Annexes. PassKit's signature of this DPA or an Agreement referencing this DPA shall be treated as signing of the 2021 EU SCCs and their Annexes. The 2021 EU SCCs shall be deemed incorporated into this DPA. Details required under the 2021 EU SCCs Annex 1 are available in Schedule 1 to this DPA, details required under the 2021 EU SCCs Annex 2 are outlined in Schedule 2 to this DPA and details required under the 2021 EU SCCs Annex 3 are outlined in Schedule 3 to this DPA. In the event of any conflict or inconsistency between this DPA and the 2021 EU SCCs the 2021 EU SCCs shall prevail.

b) **General**. The Customer shall exercise its rights pursuant to the 2021 EU SCCs acting in good faith and in a proportionate manner, and where appropriate, taking into account PassKit's expertise. To the extent legally permitted, a "binding decision" is a final, non-appealable decision of a court or regulator.

c) **2021 EU SCCs Clause 8.3 - SCCs Copy**. On request by a Data Subject, the Customer may make a copy of the 2021 EU SCCs, available to the Data Subject in accordance with Clause 8.3. Customer shall not make the entirety of this DPA available but a copy of the 2021 EU SCCs (including the relevant Schedules of this DPA) only. Customer shall make commercially reasonable efforts to consult PassKit in order to redact the 2021 EU SCCs and/or the relevant Schedules of this DPA to the extent necessary to protect PassKit's business secrets or other Confidential Information, prior to sharing them with the Data Subject. The Parties shall make good faith efforts to coordinate the response to the Data Subject regarding the reasons for the redactions, to the extent possible without revealing the redacted information.

d) **2021 EU SCCs Clause 8.4 - Accuracy.** PassKit will provide assistance to Customer to erase or rectify inaccurate Personal Data in accordance with Clause 8.4, by providing appropriate technical and organizational measures, where possible through the PassKit Services and/or as outlined in the Documentation.

e) **2021 EU SCCs Clause 8.6 - Security of Processing.** PassKit shall comply with its obligations under Clause 8.6(d) by providing commercially reasonable assistance to the Customer in relation to a Personal Data Breach, taking into account the nature of the processing and the information available to PassKit. PassKit conducts regular checks of the technical and organisational measures required by Clause 8.6 in the form of an annual ISO 27001 audit.

f) **2021 EU SCCs Clause 8.9 - Audit Rights.** Audits pursuant to Clause 8.9 of the 2021 EU SCCs shall be carried out in accordance with Section 10.3 above. In addition, in case of demonstrable indications of material non-compliance by PassKit of its processing obligations under the 2021 EU SCCs, Customer may perform an On-site Audit ("**Compliance Audit**"), in which case any On-site Audit performed pursuant to Section 10.3 (ii) (f) shall not take place any earlier than twelve months from such Compliance Audit.

g) **2021 EU SCCs Clause 9 - Sub-processors.** Section 5 and Schedule 3 of this DPA represents Customer's express consent regarding existing and new Sub-processors under Clause 9(a) of the 2021 EU SCCs. PassKit shall on request by Customer pursuant to Clause 9(c) of the 2021 EU SCCs, make a copy of the applicable 2021 EU SCCs P2P available. To the extent necessary to protect business secrets, personal data or other confidential information, PassKit and the Sub-processor may redact sections of the 2021 EU SCCs P2P prior to sharing them with Customer. PassKit shall in accordance with Clause 9(d) notify the Customer of any failure by the Sub-processor to fulfil its obligations under the 2021 EU SCCs P2P where such a failure amounts to a breach of the 2021 EU SCCs P2P that leads to PassKit being in material breach of this DPA. Any and all communications, instructions, notifications, enquiries, requests, correspondence, co-operation, and assistance needs between Customer and Sub-processors intended under the 2021 EU SCCs or 2021 EU SCCs P2P shall be made exclusively via PassKit.

h) **2021 EU SCCs Clause 14 - Transfer Impact Assessments.** Upon Customer request, PassKit will make available to Customer its documented assessment of its processing of Personal Data hereunder for the purpose of Clause 14 of the 2021 EU SCCs and the parties agree that such PassKit assessment provides to

Customer the relevant information that a data importer is required to provide to a data exporter in accordance with clause 14 (b) and clause 14 (c) of the 2021 EU SCCs.

i) **2021 EU SCCs Clauses 14 (f), 16 (b) and 16 (c) - Suspension and Termination.** Where Customer exercises any of its rights to suspend the processing of Customer Data within the PassKit Services or its right to terminate any applicable Order Form(s) pursuant to Clauses 14 (f), 16 (b) or16 (c) of the 2021 EU SCCs:

   1. Customer shall notify PassKit in writing setting forth in reasonable detail the alleged or actual material non-compliance with the requirements of the 2021 EU SCCs ("Compliance Situation") and shall provide the factual basis for such determination and identify the provisions of the 2021 EU SCCs with which, in the Customer's reasonable opinion, there is a material non-compliance by PassKit and the applicable laws and practices that are not met; ***and***

   2. without prejudice to any other rights or remedies available to either party under this DPA or otherwise, if Customer cannot implement a commercially reasonable change to its configuration or use of the PassKit Services to avoid such Compliance Situation, and if within thirty (30) days after receipt of such notice by PassKit or any other timeframe agreed by the parties, PassKit does not: (x) demonstrate that the Compliance Situation does not lead to a violation of the 2021 EU SCCs, (y) make available to Customer a change in the PassKit Services that remedies such Compliance Situation without unreasonably burdening Customer, or (z) recommend a commercially reasonable change in Customer's use or configuration of the PassKit Services that remedies such Compliance Situation without unreasonably burdening Customer; ***then***

   3. Customer may terminate the relevant Order Form(s) pursuant to the 2021 EU SCCs and Section 9.4 Termination for Cause of the Agreement. In such a case, Customer shall receive a refund of prepaid fees for the period following the effective date of termination in connection with the terminated Order Form(s) or portion thereof.

j) **2021 EU SCCs Clause 15.1 (a) - Data Subject Notification.** To the extent legally permitted, any and all communications, instructions, notifications, enquiries, requests, correspondence, co-operation, and assistance needs

between PassKit and Data Subjects intended under the 2021 EU SCCs shall be made exclusively via Customer.

k) **2021 EU SCCs Clause 15.1 (c) - Transparency Report.** PassKit regularly publishes a transparency report that provides relevant information on disclosure requests received by PassKit from public authorities and indicates whether a disclosure request was received by a Sub-processor at https://passkit.com/legal/ (the "**PassKit Transparency Report**"). The parties agree that PassKit complies with its obligations under Clause 15.1 (c) of the 2021 EU SCCs and of the corresponding Clause under the 2021 EU SCCs P2P by making such a subscription mechanism available to Customer.

11. CCPA SPECIFIC PROVISIONS

Any capitalized term used in this Section 11 but not defined herein, shall have the meaning set forth in the CCPA. The following shall apply for Customers subject to the CCPA:

11.1. All references to "Personal Data" in this DPA shall be deemed to include "Personal Information" provided such data is Customer Data, and references to "Controller" and "Processor" shall be deemed to be references to "Business" and "Service Provider" as defined in the CCPA.

11.2. PassKit will retain, use, disclose or otherwise Process Personal Data solely for the Business Purpose as set forth in Section 2.3 and shall not Sell Personal Data.

11.3. PassKit certifies that it understands the restrictions set forth in this DPA and will comply with them.

List of Schedules:

Schedule 1: Details of the Processing

Schedule 2: PassKit Security, Privacy and Architecture Datasheet

Schedule 3: List of Sub-processors Used in Connection with the PassKit Services

SCHEDULE 1

DETAILS OF THE PROCESSING

1. Nature and Purpose of Processing

PassKit will Process Personal Data as necessary to perform the PassKit Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the PassKit Services.

2. Duration of Processing

Subject to Section 7 of the DPA, PassKit will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

3. Categories of Data Subjects

Customer may submit Personal Data to the PassKit Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

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

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

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

(iv) Customer's Users authorized by Customer to use the PassKit Services

4. Type of Personal Data

Customer may submit Personal Data to the PassKit Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

(i) Email address

(ii) Device data

(iii) ID data

(iv) Personal life data (such as for example: date of birth, hobbies, city of residence)

SCHEDULE 2

PASSKIT SECURITY, PRIVACY, AND ARCHITECTURE DATASHEET

(effective as of April 2024; subject to change without notice)

Introduction

The goal of this document is to provide high-level information to our customers regarding PassKit's commitment to security and data protection.

PassKit's Corporate Trust Commitment

PassKit is committed to achieving and maintaining the trust of our customers. Our goal is to be as transparent as possible with our customers in offering state-of-the-art security and protections to meet and exceed expectations in today's modern computing world.

1. Policy Ownership

PassKit has a documented information security policy that all employees must read and acknowledge. This policy is reviewed and updated annually. Security policy development, maintenance, and issuance is the responsibility of the PassKit Security Team.

2. PassKit Infrastructure

PassKit customers may elect European or US hosting options.

For Europe-hosted customers, PassKit hosts the PassKit Services with Google Cloud in their Netherland (europe-west4) location.

For US-hosted customers, PassKit hosts the PassKit Services with Google Cloud in their Iowa (us-central1) location.

3. Third-Party Architecture

PassKit may use one or more third-party content delivery networks to provide the PassKit Services and to optimize content delivery via the PassKit Services. Content items to be served to subscribers or end-users, such as images or attachments uploaded to the PassKit Services, may be cached with such content delivery networks to expedite transmission.

Information transmitted across a content delivery network may be accessed by that content delivery network solely to enable these functions.

4. Audits, Certifications, and Regulatory Compliance

PassKit is in the process of securing SOC2 Type 1 certification.

Security Controls

5. Organization Security

PassKit's CTO is responsible for the overall security of the PassKit Services, including oversight and accountability. PassKit's contracts with third-party hosting providers such as Google Cloud and Amazon Web Services include industry-standard information protection requirements.

6. Asset Classification and Logical Access Control

PassKit maintains an inventory of essential information assets such as servers, databases, and information. All Customer Data is classified as Confidential by PassKit.

PassKit adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff. For example, Customer Success Managers only have access to the regions for which they are directly responsible. PassKit maintains separate development, staging (or sandbox), user acceptance testing, and production environments access to each environment and within each environment is strictly controlled.

Access to PassKit's servers is controlled via revocable SSH keys managed via configuration management and rotated at least annually. All access to PassKit's servers or Customer Data is logged and can only be accessed through PassKit's VPN, which uses multi-factor authentication. Database access is controlled via 32 and 64-character passwords with IP whitelisting.

PassKit's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.

7. Personnel Security and Training

All employees at PassKit sign a non-disclosure agreement when their employment begins. In addition, PassKit conducts background checks of its employees as part of its onboarding process. All employees are informed of, and agree to comply with, PassKit's security policies and practices as a part of their initial onboarding.

All PassKit employees undergo annual security and privacy training.

System administrators, developers and other users with privileged access receive special and ongoing training and are subjected to additional background screening.

8. Physical and Environmental Security

Since all PassKit employees work remotely, there is no physical PassKit facility to access. All PassKit employee workstations are encrypted and password protected, and all PassKit user accounts require two-factor authentication.

Data centers and servers are managed and controlled by our Cloud hosting providers, Google Cloud and Amazon Web Services. PassKit employees have no access to any of these data centers.

Details regarding the security practices and controls applicable to these facilities can be found at their websites:

- Google Cloud: https://cloud.google.com/security
- AWS: https://aws.amazon.com/security/

9. Policies and Logging

The PassKit Services are operated in accordance with the following procedures to enhance security:

- User passwords are never transmitted or stored in clear text
- PassKit uses industry-standard methods to determine password validity
- API key information for third-party services provided by the customer are encrypted for storage
- PassKit keeps audit logs for all access to production servers
- Server access is controlled via public key access, instead of passwords, and only permitted from devices physically connected to the PassKit office network, or securely connected to the PassKit office network via a single, secure VPN.
- Logs are stored in a secure centralized host to prevent tampering
- PassKit application and ssh audit logs are stored for one year
- Passwords are not logged under any circumstances
- Access to PassKit mail and document services is only allowed on approved mobile devices that have automated security policies enforced, such as encryption, autolock and passwords
- All access to customer dashboard accounts by PassKit Employees must be done through an internal service that is accessible only from the PassKit office network (either physically, or via a secure VPN).
- As part of PassKit's Employee Information Security Policy, employees may not store any Customer Data on removable media

10. Intrusion Detection

PassKit monitors system, user, and file behavior across its infrastructure using a host-based Intrusion Detection System. Intrusion Detection alerts are monitored by the Security and DevOps teams 24/7. Additionally, PassKit may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the PassKit Services function properly.

PassKit's APIs and Dashboard use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and automatically alert PassKit's engineering team.

11. Security Logs

All PassKit systems used in the provision of the PassKit Services, including firewalls, routers, network switches, and operating systems log information to their respective system log facility or a centralized logging service (for cloud systems) in order to enable security reviews and analysis. PassKit has automated alerts and searches on these logs.

12. System Patching and Configuration Management

PassKit patches its development servers and rebuilds its entire cloud infrastructure from configuration management systems on a regular basis, which ensures that the latest patches are applied and that we "reset" back to a known, clean state. PassKit's configuration management system regularly applies patches via Linux repositories. PassKit uses the CI/CD pipelines and Kubernetes to automate this entire process, across our entire infrastructure.

PassKit maintains multiple environments and tests changes in local development environments and in cloud-based staging environments before making changes to production environments.

13. Vulnerability Management

PassKit's infrastructure and applications are continuously scanned by a Vulnerability Management System. Alerts are monitored by our Security Team and addressed at least monthly by the PassKit Team. Patches and 'critical' and 'high' vulnerabilities are remediated no later than 30 days following discovery.

PassKit also uses static code analysis tools during the build process to perform static security analysis.

14. Third-Party Penetration Testing

Customers are granted the express right to conduct, at their own expense and risk, independent penetration testing ("Penetration Testing") of the PassKit's staging and production environments ("Environments"), on a one-time or recurring basis. Any vulnerabilities discovered during Penetration Testing shall be reported to PassKit through a ticketing system with a critical priority designation.

PassKit reserves the right to engage, at its sole discretion, certain ethical hackers who have previously identified vulnerabilities to conduct additional Penetration Testing of the Environments.

15. Monitoring

For technical monitoring, maintenance and support processes, PassKit uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring Uptime monitoring
- Functional monitoring
- Database monitoring
- APM performance monitoring
- Error monitoring
- Office monitoring

16. Customer Access Control

The PassKit Services employ a variety of security controls. These include, but are not limited to:

- All requests on the PassKit Dashboard have cross-site request forgery (CSRF) protection. All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
- PassKit does not use cookies for session storage to avoid replay attacks. Sessions expire after a few hours of inactivity.
- User passwords on the PassKit Dashboard must meet minimum password length requirements. At the customer's request, PassKit can add password complexity requirements, such as lowercase, uppercase, numeral, and special characters, and set a password expiration policy such that users must change their passwords regularly.
- User password history of the last six passwords prevents the reuse of User passwords.
- Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.

- PassKit's REST APIs are accessed with separate API keys, which can only be provisioned by PassKit dashboard user accounts with administrative access. API keys are granted access to specific API endpoints when created.

17. Development and Maintenance

PassKit uses tools such as Bitbucket, Git and Jenkins to effectively manage the development lifecycle. During testing, PassKit generates sandbox accounts and fake data for testing. PassKit does not use production data in sandbox accounts.

Application source control is accomplished through private Bitbucket repositories. PassKit has controls in place to ensure that all code must be approved before being merged to PassKit's main code branch; only the CTO and approved employees are granted access to promote code to production.

PassKit developers receive additional security training as part of their onboarding, and undergo regular and periodic security training during the term of their employment. PassKit maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

18. Malware Prevention

As a mitigating factor against malware, all PassKit servers run LTS editions of Operation Systems, as well as endpoint monitoring services such as Threat Stack, ClamAV and/or Sophos for virus and malware protection.

PassKit adopts the principle of least privilege for all accounts running application or database services. Proper change management ensures that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All PassKit employee computers have virus scanners installed and updated definitions sent out from a central device management platform.

19. Information Security Incident Management

PassKit maintains written and regularly-audited security incident management policies and procedures, including an Incident Response Plan to be enacted in the event of an incident.

20. Data Encryption

The PassKit Services use industry-accepted encryption practices to protect Customer Data and communications during transmissions between a customer's network and the PassKit Services, including 256-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

PassKit audits the TLS ciphers used in connection with the provision of the PassKit Services with third-party security auditors to ensure that anonymous or weak ciphers are not used. These audits also confirm that the PassKit Services do not allow client renegotiation, support downgrade attack protection and forward secrecy.

Data shipped to Google Cloud is encrypted in transit and at-rest using AES-256 encryption via Google’s managed encryption key process.

Where use of the PassKit Services requires a customer to provide access to third party services (for example, AWS S3 credentials for data exports), PassKit performs additional encryption of that information.

21. Return and Deletion of Customer Data

The PassKit Services allow import, export, and deletion of Customer Data by authorized users at all times during the term of a customer’s subscription. Following termination or expiration of the PassKit Services, PassKit shall securely overwrite or delete Customer Data within 60 days following any such termination, in accordance with the Agreement, applicable laws and the Documentation.

22. Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the PassKit Services is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

23. Business Continuity Management and Disaster Recovery

PassKit has a written Business Continuity and Disaster Recovery Plan, which is tested annually. PassKit tests database backups and failovers as part of our Business Continuity Plan. Backups are encrypted and stored in Google Cloud and Amazon Web Services provided backup services.

24. Mobile Device Management Policies

PassKit uses Mobile Device Management ("MDM") platforms to control and secure access to PassKit resources on mobile devices such as phones, tablets, and laptops. PassKit uses Apple for its phone and tablet MDM policy, and enforces common security settings such as, but not limited to, encryption, lock screen passwords, password expiration and display timeouts.

25. Blocking Third Party Access

The PassKit Services have not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access Customer Data. We do not voluntarily provide any government or other third party with encryption keys, or any other way to break our encryption.

26. Contacts

PassKit's Security Team can be reached by emailing security@PassKit.com.

SCHEDULE 3

LIST OF SUB-PROCESSORS
USED IN CONNECTION WITH THE PASSKIT SERVICES

This Schedule describes the Sub-processors material to PassKit's provision of the PassKit Services.
(effective as of the Effective Date; subject to change)

Last Modified: July 2022

PassKit, Inc. ("PassKit") uses certain Sub-processors, whether third parties or subsidiaries of PassKit (as described below) and third parties, who process Personal Data on behalf of PassKit and in connection with PassKit's provision of the PassKit Services to its customers. Capitalized terms used herein without definition are used as defined in the Agreement.

Sub-processors are subject to written agreements that contain confidentiality and security commitments, in substance the same as those in the DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. PassKit remains responsible for the acts and omissions of its Sub-processors pursuant to the DPA.

What follows is the list of Sub-processors that PassKit uses in its provision of the PassKit Services. Depending upon a Customer's use of the PassKit Services e.g. geographical location of the Customer, not all Sub-Processors will be needed to deliver the PassKit Services. Sub-processors receive, store, structure, categorize, analyze, handle, process and send Personal Data, as applicable and in accordance with the Agreement. The Sub-processors Process Personal Data until the earlier of (i) the completion of the Processing provided by such Sub-processor, and (ii) the duration of the Agreement, subject to the terms of the Agreement and the Documentation.

Customers shall provide appropriate contact details through PassKit's applicable subscription mechanism in order to receive notice of new Sub-processors.

EU data center cloud service Infrastructure Subprocessors

Entity Name	Services Provided	Location of Processing	Security and Privacy Information	Safeguards for transfer outside of the EEA
Google Inc.	Google Cloud Platform: Third Party cloud hosting and backup for the EU instance of the PassKit Service	European Union	https://cloud.google.com/terms/data-processing-terms https://cloud.google.com/terms/subprocessors	N/A

US data center cloud service Infrastructure Subprocessors

(for customers that request the US data center)

Entity Name	Services Provided	Location of Processing	Security and Privacy Information	Safeguards for transfer outside of the EEA
Google Inc.	Google Cloud Platform: Third Party cloud hosting and backup for the EU instance of the PassKit Service	United States	https://cloud.google.com/terms/data-processing-terms https://cloud.google.com/terms/subprocessors	EU Standard Contractual Clauses

Service Specific Subprocessors - for both EU Cloud Service and US Cloud Service

PassKit works with certain Subprocessors in connection with the delivery, operations and troubleshooting of the PassKit Service and related support to customers. In order to provide the relevant functionality these Subprocessors may process Customer Data.

Entity Name	Services Provided	Location of Processing	Security and Privacy Information	Safeguards for transfer outside of the EEA
Amazon Web Services, Inc.	Amazon SES (Simple Email Service): Third Party email delivery service	United States	https://docs.aws.amazon.com/ses/latest/dg/data-protection.html	EU Standard Contractual Clauses
Intercom R&D Unlimited Company	Intercom Subscription: Third party customer support service	United States	https://www.intercom.com/legal/security-policy	EU Standard Contractual Clauses
Calendly LLC	Calendly Subscription: Appointment booking and management service	United States	https://calendly.com/security	EU Standard Contractual Clauses
Amazon Web Services, Inc.	Amazon S3 and Amazon Cloudfront used for website and web-app hosting.	United States	https://docs.aws.amazon.com/AmazonS3/latest/userguide/DataDurability.html https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/data-protection-summary.html	EU Standard Contractual Clauses
Apple, Inc.	Push Message Services for Apple Wallet	United States	https://www.apple.com/legal/privacy/data/en/wallet/	EU Standard Contractual Clauses
Google, Inc.	Google Wallet Services	United States	https://safety.google/security-privacy/	EU Standard Contractual Clauses