LOOPY LOYALTY DATA PROCESSING ADDENDUM

Version: 2026.06
Effective Date: June 2026

This Data Processing Addendum ("DPA") forms part of the Loopy Loyalty Terms and Conditions or other written or electronic agreement between PassKit, Inc. and Customer (the "Agreement") for the purchase or use of the Loopy Loyalty services (the "Services" or "Loopy Loyalty Services").

Loopy Loyalty is a product and service owned and operated by PassKit, Inc. For the purposes of this DPA, PassKit, Inc. is referred to as "PassKit", "we", "us" or "Processor", as applicable.

In the event of conflict between this DPA and the Agreement with respect to the Processing of Personal Data, this DPA shall prevail.

By entering into 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 in this DPA shall have the meaning given to them in the Agreement.

In the course of providing the Loopy Loyalty Services to Customer pursuant to the Agreement, PassKit will Process Personal Data on behalf of Customer. The Parties agree to comply with the following provisions with respect to such Personal Data, each acting reasonably and in good faith.

For the avoidance of doubt, each reference to 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 in connection with the Loopy Loyalty Services.

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, the United Kingdom, or Switzerland; and (ii) is permitted to use the Loopy Loyalty 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 amended from time to time.

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

“Customer Data” means the data submitted to, stored in, or otherwise processed through the Loopy Loyalty Services by or on behalf of Customer, including data submitted by Customer’s Users or End-Users.

“Data Protection Laws and Regulations” means all laws and regulations applicable to a party in its use or provision of the Loopy Loyalty Services in connection with the Processing of Personal Data, privacy and/or electronic communications under the Agreement, including, where applicable:

(i) the Data Protection Act 2018;
(ii) the UK General Data Protection Regulation (“UK GDPR”);
(iii) Regulation (EU) 2016/679, the General Data Protection Regulation (“GDPR”);
(iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003;
(v) the Swiss Federal Act on Data Protection of 25 September 2020, as revised and in force as of 1 September 2023 (“FADP”), including its implementing ordinances; and
(vi) the CCPA.

“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 rights to access, rectify, restrict the Processing of Personal Data, erase Personal Data, data portability, object to Processing, or not be subject to automated individual decision-making.

“EEA” means the European Economic Area.

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

“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.

“Processing” means any operation or set of operations performed upon Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction.

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

“Security, Privacy and Architecture Datasheet” means the security, privacy and architecture information for the Loopy Loyalty Services set out in Schedule 2, as updated from time to time.

“Security Measures” means the technical and organizational measures implemented by PassKit to protect Customer Data, as detailed in Schedule 2.

“Sub-processor” means any Processor engaged by PassKit or its Affiliates in connection with the Processing of Personal Data.

“UK Addendum” means the International Data Transfer Addendum to the 2021 EU SCCs issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018.

“2021 EU Standard Contractual Clauses” or **“2021 EU SCCs”** means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, issued by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

“2021 EU SCCs P2P” means the Processor-to-Processor modules of the 2021 EU SCCs that PassKit may enter into with its Sub-processors.

Where the FADP applies to the Processing of Personal Data under this DPA, any reference to the GDPR shall be interpreted, mutatis mutandis, as a reference to the corresponding provision of the FADP.

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 PassKit or its Affiliates may engage Sub-processors pursuant to Section 5.

The subject matter of Processing of Personal Data by PassKit is the performance of the Loopy Loyalty Services pursuant to the Agreement. The duration of the Processing, nature and purpose of Processing, types of Personal Data and categories of Data Subjects are further specified in Schedule 1.

This DPA shall remain in force for the term of the Agreement and for as long as PassKit retains Personal Data on behalf of Customer.

2.2. **Customer's Processing of Personal Data**

Customer shall, in its use of the Loopy Loyalty Services, Process Personal Data in accordance with Data Protection Laws and Regulations. 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 entry into the Agreement, Customer's complete and final documented instructions to PassKit for the Processing of Personal Data. Customer's configuration and use of the Loopy Loyalty Services shall constitute additional instructions to PassKit.

Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquired 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 forms;

(ii) Processing initiated by Users in their use of the Loopy Loyalty Services; and

(iii) Processing to comply with other documented reasonable instructions provided by Customer, where such instructions are consistent with the Agreement.

PassKit will Process Personal Data in compliance with applicable Data Protection Laws and Regulations, provided that PassKit shall not be in breach of this obligation where PassKit's non-compliance is caused by Customer's instructions, Customer's data, or Customer's use of the Loopy Loyalty Services.

If PassKit determines the purposes and means of any Processing of Personal Data other than as permitted under this DPA and the Agreement, PassKit shall be considered a Controller in respect of that Processing.

3. RIGHTS OF DATA SUBJECTS

3.1. Data Subject Requests

PassKit shall, to the extent legally permitted and to the extent PassKit is able to identify that the request relates to Personal Data submitted to the Loopy Loyalty 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.

PassKit may confirm to the Data Subject that it has passed the request to Customer, but PassKit shall not independently handle or execute the Data Subject Request unless required by applicable law or instructed by Customer.

3.2. Assistance

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 Data Subject Requests 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 Personal Data, have received appropriate training on their responsibilities, and are subject to confidentiality obligations.

4.2. Reliability

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

4.3. Limitation of Access

PassKit shall ensure that access to Personal Data is limited to personnel who require such access to provide, maintain, secure or support the Loopy Loyalty Services in accordance with the Agreement.

4.4. Data Protection Contact

PassKit may be contacted regarding privacy and data protection matters at:

privacy@passkit.com

Security matters and suspected security incidents may be reported to:

security@passkit.com

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors

Customer acknowledges and agrees that:

(i) PassKit's Affiliates may be retained as Sub-processors; and

(ii) PassKit and its Affiliates may engage third-party Sub-processors in connection with the provision, operation, support and improvement of the Loopy Loyalty Services.

PassKit shall enter into a written agreement with each Sub-processor containing data protection obligations that are, in substance, no less protective than those in this DPA, to the extent applicable to the nature of the services provided by such Sub-processor.

5.2. Current Sub-processors and Notification of New Sub-processors

Schedule 3 contains a current list of Sub-processors material to the provision of the Loopy Loyalty Services.

PassKit will notify Customer of any new Sub-processor at least thirty (30) calendar days before authorizing such new Sub-processor to Process Personal Data in connection with the Loopy Loyalty Services. Such notice may be provided through an applicable subscription mechanism, website notice, email notice, or other reasonable means.

5.3. Objection Right for New Sub-processors

Customer may object to PassKit's use of a new Sub-processor by notifying PassKit in writing within ten (10) calendar days after receipt of PassKit's notice.

If Customer objects to a new Sub-processor, PassKit will use reasonable efforts to make available to Customer a change in the Loopy Loyalty Services or recommend a commercially reasonable change to Customer's configuration or use of the Loopy Loyalty 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, not exceeding thirty (30) days, Customer may terminate the applicable portion of the Loopy Loyalty Services that cannot be provided without the objected-to new Sub-processor. PassKit will refund Customer any prepaid fees covering the remainder of the term for the terminated portion of the Services.

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 this DPA.

6. SECURITY

6.1. Controls for the Protection of Customer Data

PassKit shall maintain appropriate technical and organizational measures for the protection of the security, confidentiality and integrity of Customer Data, including protection against Personal Data Breaches, as set out in Schedule 2.

Customer is responsible for reviewing the information made available by PassKit relating to data security and making an independent determination as to whether the Loopy Loyalty Services meet Customer's requirements and legal obligations.

Customer acknowledges that the Security Measures are subject to technical progress and development and that PassKit may update or modify such measures from time to time, provided that such updates and modifications do not result in a material decrease in the overall security of the Loopy Loyalty Services during the applicable subscription term.

6.2. Personal Data Incident Management and Notification

PassKit maintains security incident management policies and procedures. PassKit shall notify Customer without undue delay and, in any event, no later than twenty-four (24) hours 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, taking into account the nature of Processing and the information available to PassKit.

Such information may include, where available:

(i) a description of the nature of the Personal Data Breach;

(ii) the categories and approximate number of Data Subjects concerned;

(iii) the categories and approximate number of Personal Data records concerned;

(iv) the likely consequences of the Personal Data Breach; and

(v) the measures taken or proposed to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

PassKit shall make commercially reasonable efforts to identify the cause of a Personal Data Breach and take such steps as PassKit deems necessary and reasonable to remediate the cause, to the extent remediation is within PassKit's reasonable control.

This obligation shall not apply to Personal Data Breaches caused by Customer, Customer's Users, or Customer's systems.

6.3. Audits, Certification and Reports

PassKit, Inc. maintains a SOC 2 Type 2 report covering relevant corporate controls, security processes, infrastructure management and supporting systems used in the operation of its products and services.

Loopy Loyalty is operated under PassKit's security programme; however, Loopy Loyalty is not separately represented as SOC 2 certified unless expressly stated by PassKit in writing.

Upon Customer's written request at reasonable intervals, and subject to applicable confidentiality obligations, PassKit shall make available to Customer information reasonably necessary to demonstrate compliance with this DPA. This may include applicable security documentation, summaries, third-party reports or certifications that PassKit makes available to customers generally.

7. RETURN AND DELETION OF CUSTOMER DATA

The Loopy Loyalty Services allow export and deletion of Customer Data during the subscription term.

At termination or expiration of the Agreement, PassKit shall return Customer Data by enabling Customer to export 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 Customer, PassKit will provide a certificate or written confirmation of deletion once Customer Data has been deleted from the Loopy Loyalty Services.

PassKit shall delete Customer Data within sixty (60) days following termination or expiration of the Agreement, unless retention is required by applicable law.

8. AFFILIATES

8.1. Relationship between PassKit and Customer's Authorized Affiliates

The Parties acknowledge and agree that, by entering into the Agreement, 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 DPA.

Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement.

For clarity, an Authorized Affiliate does not become a party to the Agreement and is only a party to this DPA. All access to and use of the Loopy Loyalty Services by

Authorized Affiliates must comply with the Agreement, and any violation by an Authorized Affiliate shall be deemed a violation by Customer.

8.2. **Communication**

Customer shall remain responsible for coordinating all communication with PassKit under this DPA and shall 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 Data Protection Laws and Regulations, be entitled to exercise rights and seek remedies under this DPA, subject to the following:

(i) unless applicable law requires otherwise, Customer shall exercise any such right or seek any such remedy on behalf of such Affiliate or Authorized Affiliate;

(ii) Customer shall exercise such rights in a combined manner for all relevant Affiliates and Authorized Affiliates; and

(iii) when carrying out any audit or request, Customer shall take reasonable measures to limit any impact on PassKit and its Sub-processors.

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, whether in contract, tort or under any other theory of liability, shall be subject to the limitations of liability set forth in the Agreement.

10. UK, EU & SWISS SPECIFIC PROVISIONS

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

10.1. **Data Protection Impact Assessment**

Upon Customer's request, PassKit shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation to carry out a data protection impact assessment related to Customer's use of the Loopy Loyalty 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 cooperation or prior consultation with a supervisory authority, to the extent required under Data Protection Laws and Regulations.

10.2. **Infringing Instructions**

PassKit shall inform Customer if, in PassKit's opinion, an instruction infringes applicable Data Protection Laws and Regulations.

10.3. **Audit right**

To minimize the need for on-site audits and recognizing PassKit's commitment to data security, PassKit will make available relevant security documentation and, where applicable, third-party reports or certifications.

PassKit shall allow for and contribute to audits and inspections not more than once per year, primarily through provision of available security information, reports and documentation.

Any audit shall be subject to reasonable notice, confidentiality obligations, and reasonable limitations designed to protect the security, confidentiality and availability of PassKit's systems and the data of other customers.

10.4. **Transfer Mechanisms 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, the United Kingdom, or Switzerland to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws and Regulations, PassKit makes available the following transfer mechanisms, which shall apply in the order of precedence below:

(i) any valid transfer mechanism pursuant to applicable EU, UK or Swiss Data Protection Laws and Regulations to which PassKit subscribes, certifies or participates; and

(ii) the 2021 EU SCCs and/or the UK Addendum, when available and valid under applicable Data Protection Laws and Regulations.

For transfers of Personal Data subject to the UK GDPR, the UK Addendum shall apply to and form part of the 2021 EU SCCs in accordance with its terms.

Where Customer or an Authorized Affiliate is the data exporter, Customer's entry into this DPA or an Agreement referencing this DPA shall be treated as signing of the 2021 EU SCCs and their annexes. PassKit's entry into 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 Annex I of the 2021 EU SCCs are set out in Schedule 1. Details required under Annex II are set out in Schedule 2. Details required under Annex III are set out in Schedule 3.

In the event of conflict or inconsistency between this DPA and the 2021 EU SCCs, the 2021 EU SCCs shall prevail.

10.5. **Additional SCC Provisions**

The Parties agree as follows:

(i) Customer shall exercise its rights under the 2021 EU SCCs acting in good faith and in a proportionate manner.

(ii) On request by a Data Subject, Customer may make a copy of the 2021 EU SCCs available to the Data Subject, subject to redaction of confidential or commercially sensitive information.

(iii) PassKit will provide assistance to Customer to erase or rectify inaccurate Personal Data by providing appropriate technical and organizational measures where possible through the Loopy Loyalty Services.

(iv) PassKit shall provide commercially reasonable assistance to Customer in relation to a Personal Data Breach, taking into account the nature of Processing and information available to PassKit.

(v) Audits under Clause 8.9 of the 2021 EU SCCs shall be carried out in accordance with Section 10.3.

(vi) Section 5 and Schedule 3 represent Customer's authorization regarding existing and new Sub-processors under Clause 9 of the 2021 EU SCCs.

(vii) Upon Customer request, PassKit will make available information reasonably necessary for Customer to conduct a transfer impact assessment.

(viii) Any communication, notification, enquiry, request, cooperation or assistance between PassKit and Data Subjects under the 2021 EU SCCs shall be made through Customer to the extent legally permitted.

Where the 2021 EU SCCs are relied upon for transfers of Personal Data subject to the FADP, the Parties agree that:

(i) references to "Member State" shall be interpreted to include Switzerland;

(ii) references to "GDPR" shall be interpreted as references to the FADP, where applicable;

(iii) the Swiss Federal Data Protection and Information Commissioner shall be the competent supervisory authority, where applicable; and

(iv) the term "EU" shall include Switzerland for purposes of Data Subject rights under the 2021 EU SCCs.

11. CCPA SPECIFIC PROVISIONS

Any capitalized term used in this Section 11 but not defined in this DPA shall have the meaning set forth in the CCPA.

Where the CCPA applies:

11.1. **Personal Information**

All references to "Personal Data" shall be deemed to include "Personal Information", provided such data is Customer Data.

References to "Controller" and "Processor" shall be deemed to refer to "Business" and "Service Provider", as applicable.

11.2. **Service Provider Obligations**

PassKit will retain, use, disclose or otherwise Process Personal Data solely for the business purposes described in Section 2.3 and shall not Sell or Share Personal Data, as those terms are defined under the CCPA.

11.3. **Certification**

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: Loopy Loyalty Security, Privacy and Architecture Datasheet

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

SCHEDULE 1

DETAILS OF THE PROCESSING

1. Nature and Purpose of Processing

PassKit will Process Personal Data as necessary to provide, operate, secure, maintain, support and improve the Loopy Loyalty Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Loopy Loyalty Services.

The Loopy Loyalty Services enable Customer to create, manage and operate digital loyalty programmes, including digital stamp cards, customer enrolment, loyalty activity, reward redemption, messaging and related analytics.

2. Duration of Processing

Subject to Section 7 of this DPA, PassKit will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing or required by applicable law.

3. Categories of Data Subjects

Customer may submit Personal Data to the Loopy Loyalty Services, the extent of which is determined and controlled by Customer in its sole discretion. Categories of Data Subjects may include:

(i) Customer's end customers, loyalty programme members and prospective customers;

(ii) individuals who enrol in or interact with a Customer loyalty programme;

(iii) employees, contractors, agents or representatives of Customer;

(iv) Customer's authorized Users of the Loopy Loyalty Services;

(v) employees or contact persons of Customer's business partners, vendors or service providers; and

(vi) other individuals whose Personal Data is submitted to the Loopy Loyalty Services by or on behalf of Customer.

4. Type of Personal Data

Customer may submit Personal Data to the Loopy Loyalty Services, the extent of which is determined and controlled by Customer in its sole discretion. Such Personal Data may include:

(i) name;

(ii) email address;

(iii) phone number, where configured by Customer;

(iv) date of birth, where configured by Customer;

(v) postcode, city, country or similar location information, where configured by Customer;

(vi) loyalty card identifiers and membership identifiers;

(vii) loyalty activity, including stamps, visits, rewards, redemptions and transaction history;

(viii) wallet pass information and device-related data required to provide Apple Wallet or Google Wallet functionality;

(ix) marketing preferences and consent records, where configured by Customer;

(x) signup form responses and custom fields configured by Customer;

(xi) technical data, such as IP address, browser information, device type, operating system, logs and usage data; and

(xii) other Personal Data submitted by Customer or Customer's Users.

5. Special Categories of Personal Data

The Loopy Loyalty Services are not designed for the Processing of special categories of Personal Data. Customer shall not submit special categories of Personal Data to the Loopy Loyalty Services unless Customer has a lawful basis to do so and has configured the Services appropriately.

6. Frequency of Processing

Processing is continuous for the duration of Customer's use of the Loopy Loyalty Services.

7. Subject Matter of Processing

The subject matter of Processing is the provision of the Loopy Loyalty Services by PassKit to Customer under the Agreement.

8. Roles of Parties

Customer is the Controller of Personal Data. PassKit is the Processor of Personal Data.

SCHEDULE 2

LOOPY LOYALTY SECURITY, PRIVACY & ARCHITECTURE DATASHEET

Introduction

This Schedule provides high-level information regarding PassKit's security, privacy and architecture practices as they relate to the Loopy Loyalty Services.

Loopy Loyalty is owned and operated by PassKit, Inc. PassKit is committed to maintaining appropriate technical and organizational measures designed to protect Customer Data against unauthorized access, loss, misuse, alteration and disclosure.

1. Corporate Trust Commitment

PassKit is committed to achieving and maintaining the trust of its customers. PassKit's security programme is designed to provide administrative, technical and organizational controls appropriate to the nature of the Services and the Personal Data processed.

PassKit, Inc. maintains a SOC 2 Type 2 report covering relevant corporate controls, security processes, infrastructure management and supporting systems used in the operation of its products and services. Loopy Loyalty is operated under PassKit's security programme; however, Loopy Loyalty is not separately represented as SOC 2 certified unless expressly stated by PassKit in writing.

2. Policy Ownership

PassKit maintains documented information security policies that employees are required to acknowledge. These policies are reviewed and updated periodically.

Security policy development, maintenance and oversight are the responsibility of PassKit's Security Team and senior technical leadership.

3. Infrastructure

Loopy Loyalty is currently hosted using a combination of Amazon Web Services ("AWS") and IBM Cloud services in the United States.

AWS services are used for application hosting, compute, storage, content delivery, backups, email delivery infrastructure and related platform functions. IBM Cloudant is used as a managed database service supporting the Loopy Loyalty platform.

Loopy Loyalty customer data is currently hosted and processed in the United States. Customers do not currently select a hosting region for the Loopy Loyalty Services.

Infrastructure architecture may evolve over time as part of PassKit's ongoing operational and technical improvements, including migration to alternative cloud

platforms such as Google Cloud Platform where appropriate. PassKit may update infrastructure and Sub-processors in accordance with this DPA.

4. Third-Party Architecture

PassKit may use third-party content delivery networks, hosting providers, managed database services, analytics providers, wallet platform providers, payment processors, email delivery providers and customer support tools to provide, support and optimize the Loopy Loyalty Services.

Content items served to subscribers or end-users, such as images, digital pass assets or attachments uploaded to the Loopy Loyalty Services, may be cached or transmitted via such providers to expedite delivery and ensure service availability.

5. Organization Security

PassKit's technical leadership is responsible for oversight and accountability for the security of the Loopy Loyalty Services.

PassKit's contracts with relevant third-party hosting and infrastructure providers include information protection requirements appropriate to the services provided.

6. Asset Classification and Logical Access Control

PassKit maintains an inventory of essential information assets. Customer Data is treated as confidential.

PassKit applies the principle of least privilege to accounts used for application, database, infrastructure and administrative access.

PassKit maintains separate development, staging or testing, and production environments where appropriate. Access to production environments is limited to authorized personnel with a business need.

Access to production infrastructure and Customer Data is logged and restricted using security controls such as VPN, multi-factor authentication, access management and credential rotation, as appropriate.

PassKit's onboarding and offboarding processes are designed to provision and de-provision access based on role and employment status.

7. Personnel Security and Training

PassKit personnel are subject to confidentiality obligations. Employees receive security and privacy training as part of onboarding and periodically thereafter.

Personnel with privileged access receive additional guidance and are expected to comply with PassKit security policies and procedures.

8. Physical and Environmental Security

PassKit operates as a remote-first organization. PassKit employees do not have physical access to the data centres operated by its cloud infrastructure providers.

Physical and environmental security controls for data centres and cloud infrastructure are managed by PassKit's cloud hosting providers, including AWS and IBM Cloud.

PassKit employee workstations are required to use appropriate security controls, such as device encryption, password protection, screen locking and access controls.

9. Policies and Logging

The Loopy Loyalty Services are operated in accordance with procedures designed to enhance security, including:

(i) passwords are not stored or transmitted in clear text;

(ii) industry-standard methods are used to validate passwords;

(iii) API keys and sensitive credentials are protected;

(iv) access to production systems is logged;

(v) logs are maintained to support security review and investigation;

(vi) passwords are not intentionally logged;

(vii) access to customer accounts by PassKit personnel is restricted to authorized personnel with a business need; and

(viii) employees may not store Customer Data on removable media except as expressly authorized under PassKit policy.

10. Intrusion Detection

PassKit monitors systems, users and infrastructure behaviour using security monitoring tools and procedures.

Alerts relating to suspicious activity, unauthorized access attempts, abnormal system behaviour or service availability may be reviewed by PassKit's Security, Engineering or DevOps teams.

PassKit may process technical information such as device type, browser type, operating system, IP address, time zone and usage data for security purposes, including fraud prevention, authentication protection, abuse prevention and ensuring the Services function properly.

11. Security Logs

Systems used in the provision of the Loopy Loyalty Services may generate logs to enable security review, troubleshooting, auditing and operational monitoring.

Access to logs is restricted to authorized personnel. Logs may be retained for a reasonable period for security, operational and compliance purposes.

12. System Patching and Configuration Management

PassKit uses configuration management, automated deployment processes and patching procedures to maintain infrastructure and application security.

PassKit tests changes in development, staging or testing environments, where appropriate, before production deployment.

Critical and high-risk vulnerabilities are prioritized for remediation based on severity, exploitability and potential impact.

13. Vulnerability Management

PassKit uses vulnerability management processes to identify, assess and remediate security vulnerabilities.

PassKit may use vulnerability scanning, dependency scanning, code review, static analysis and other security testing processes as part of its software development lifecycle.

14. Penetration Testing

PassKit may engage independent security professionals to conduct security assessments of its environments.

Customers may request to conduct independent penetration testing of the Loopy Loyalty Services, subject to PassKit's prior written approval and the following conditions:

(i) Customer must provide at least thirty (30) days' prior written notice describing the proposed scope, methodology, timing and duration;

(ii) the scope and timing must be mutually agreed in writing;

(iii) testing must not include denial-of-service, stress or load testing;

(iv) testing must not attempt to access data belonging to other customers;

(v) testing must not disrupt PassKit's services or infrastructure;

(vi) testing must not include social engineering, phishing simulations or physical security testing;

(vii) all findings must be treated as Confidential Information and promptly provided to PassKit; and

(viii) any vulnerabilities discovered must be reported to PassKit without undue delay.

PassKit reserves the right to monitor, suspend or terminate testing that it reasonably determines may threaten the security, availability or integrity of its systems.

15. Monitoring

PassKit uses technical monitoring, maintenance and support processes to ensure the Loopy Loyalty Services are operating properly. Monitoring may include:

(i) process monitoring;

(ii) CPU, disk and memory monitoring;

(iii) uptime monitoring;

(iv) functional monitoring;

(v) database monitoring;

(vi) application performance monitoring;

(vii) error monitoring; and

(viii) alerting for availability or performance issues.

16. Customer Access Control

The Loopy Loyalty Services employ access control measures, including:

(i) encrypted HTTPS traffic;

(ii) HTTP Strict Transport Security where applicable;

(iii) user authentication controls;

(iv) account lockout or protective measures following repeated failed login attempts where applicable;

(v) role-based access controls;

(vi) administrative restrictions for API key provisioning; and

(vii) session management controls.

Customer is responsible for managing its Users, access rights, account credentials and configuration of the Loopy Loyalty Services.

17. Development and Maintenance

PassKit uses software development lifecycle controls to manage development and release of the Loopy Loyalty Services.

These controls may include:

(i) version control;

(ii) code review;

(iii) approval workflows;

(iv) automated build and deployment processes;

(v) separate development and production environments; and

(vi) testing before production deployment.

PassKit does not intentionally use production Customer Data in development or testing environments unless required for support, troubleshooting or other legitimate operational purposes and subject to appropriate controls.

18. Malware Prevention

PassKit applies malware prevention and endpoint security measures to employee devices and infrastructure where appropriate.

PassKit uses least privilege access controls and change management practices to reduce the risk of unauthorized software installation or malicious code execution.

19. Information Security Incident Management

PassKit maintains security incident management policies and procedures, including an incident response process.

Security incidents are reviewed, triaged and remediated based on severity and impact.

Personal Data Breaches are handled in accordance with Section 6.2 of this DPA.

20. Data Encryption

The Loopy Loyalty Services use industry-accepted encryption practices to protect Customer Data and communications during transmission, including TLS for data transmitted between Customer systems, end-user devices and the Loopy Loyalty Services.

Where supported by the applicable infrastructure provider, Customer Data is encrypted at rest using provider-managed encryption or equivalent controls.

Sensitive credentials and API keys are protected using appropriate encryption or access control mechanisms.

21. Return and Deletion of Customer Data

The Loopy Loyalty Services allow authorized users to import, export and delete Customer Data during the subscription term.

Following termination or expiration of the Services, PassKit shall delete or securely overwrite Customer Data within sixty (60) days, unless retention is required by law or permitted under the Agreement.

22. Reliability and Backup

PassKit uses redundancy, backup and recovery measures appropriate to the Loopy Loyalty Services and underlying infrastructure.

Customer Data is backed up on a regular basis. Backups are protected using appropriate security controls, including encryption where supported by the relevant infrastructure provider.

23. Business Continuity Management and Disaster Recovery

PassKit maintains business continuity and disaster recovery planning appropriate to its operations and the Loopy Loyalty Services.

PassKit tests or reviews backup and recovery processes periodically.

24. Mobile Device Management Policies

PassKit uses device management and endpoint controls to secure access to PassKit resources on employee devices, including controls such as encryption, password protection, lock screen requirements and access management.

25. Blocking Third Party Access

The Loopy Loyalty Services are not designed to include backdoors or similar functionality that would allow governments or third parties to access Customer Data.

PassKit does not voluntarily provide any government or third party with encryption keys or other means to bypass its security controls, except where legally compelled.

26. Contacts

Privacy and DPA matters: privacy@passkit.com

Security matters and suspected security incidents: security@passkit.com

SCHEDULE 3

LIST OF SUB-PROCESSORS USED IN CONNECTION WITH THE LOOPY LOYALTY SERVICES

This Schedule describes the Sub-processors material to PassKit's provision of the Loopy Loyalty Services.

Last Updated: June 2026

PassKit uses certain Sub-processors, whether third-party service providers or Affiliates, who may Process Personal Data on behalf of PassKit in connection with the provision, operation, support, security, billing, analytics and improvement of the Loopy Loyalty Services.

Sub-processors are subject to written agreements that contain confidentiality and security commitments appropriate to the nature of the services provided.

Depending on Customer's use of the Loopy Loyalty Services, not all Sub-processors will Process Personal Data for every Customer.

Loopy Loyalty customer data is currently hosted and processed in the United States. Customers do not currently select a hosting region for the Loopy Loyalty Services.

1. Cloud Infrastructure Sub-Processors

Entity Name	Services Provided	Location of Processing	Security and Privacy Information	Safeguards for transfer outside of the EEA
Amazon Web Services, Inc.	Cloud infrastructure, application hosting, compute, object storage, content delivery, backup infrastructure, and related hosting services, including AWS EC2, RDS, S3 and CloudFront	United States	https://aws.amazon.com/security/ and https://aws.amazon.com/compliance/	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
IBM Corporation / IBM Cloud	IBM Cloudant managed database service supporting the Loopy Loyalty backend	United States	https://www.ibm.com/cloud/security and applicable IBM Cloud data processing terms	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum

2. Service-Specific Sub-Processors

Entity Name	Services Provided	Location of Processing	Security and Privacy Information	Safeguards for transfer outside of the EEA
Amazon Web Services, Inc.	Amazon SES email delivery services	United States	https://docs.aws.amazon.com/ses/latest/dg/data-protection.html	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
Intercom R&D Unlimited Company	Customer support and customer communications platform	United States and other locations used by Intercom	https://www.intercom.com/legal/security	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
Calendly, LLC	Appointment booking and scheduling services	United States	https://calendly.com/security	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
Stripe, Inc.	Payment processing, subscription billing and payment-related services	United States and other locations used by Stripe	https://stripe.com/docs/security and https://stripe.com/privacy	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
Brevo SAS	Email marketing, transactional email and customer communications	European Union and other locations used by Brevo	https://www.brevo.com/legal/privacypolicy/	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
Apple Inc.	Apple Wallet services, including pass distribution and push message services for Apple Wallet	United States and other locations used by Apple	https://www.apple.com/legal/privacy/	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
Google LLC	Google Wallet services and related wallet functionality	United States and other locations used by Google	https://safety.google/security-privacy/	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum
Google LLC	Google Analytics website and usage analytics	United States and other locations used by Google	https://privacy.google.com/businesses/compliance/	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum

Entity Name	Services Provided	Location of Processing	Security and Privacy Information	Safeguards for transfer outside of the EEA
Microsoft Corporation	Microsoft Clarity website analytics and usability monitoring	United States and other locations used by Microsoft	https://privacy.microsoft.com/	EU Standard Contractual Clauses, as adapted for Switzerland where applicable, and UK Addendum

3. Updates to Sub-Processors

PassKit may update this list from time to time in accordance with Section 5 of this DPA.

Customers may receive notice of new Sub-processors through an applicable subscription mechanism, website notice, email notice or other reasonable means.