EpassCard LLC
1209 Mountain Road Pl NE, Ste R
Albuquerque, NM 87110, United States
www.epasscard.com · privacy@epasscard.com

EpassCard Data Processing Agreement

UK GDPR and EU GDPR
Version 1.0, 19 November 2026

Between the Customer named in the signature block (the "**Controller**") and **EpassCard LLC**, 1209 Mountain Road Pl NE, Ste R, Albuquerque, NM 87110, United States ("**EpassCard**" or the "**Processor**").

This Data Processing Agreement ("**DPA**") forms part of the EpassCard Terms and Conditions at https://www.epasscard.com/terms-and-conditions/ (the "**Terms**"). If this DPA and the Terms conflict on personal data, this DPA prevails.

1. Definitions

1.1 "**Data Protection Law**" means the UK GDPR and the Data Protection Act 2018, as amended (including by the Data (Use and Access) Act 2025), and, where it applies, Regulation (EU) 2016/679 (the "**EU GDPR**").

1.2 "**Customer Personal Data**" means personal data that EpassCard processes on behalf of the Customer in providing the Services, as described in Annex 1.

1.3 "**Services**" means the EpassCard platform for creating, issuing, delivering and updating Apple Wallet and Google Wallet passes, with its apps, API and integrations.

1.4 "**Sub-processor**" means a third party engaged by EpassCard to process Customer Personal Data.

1.5 "**Restricted Transfer**" means a transfer of Customer Personal Data from the UK or the EEA to a country that does not benefit from adequacy regulations or an adequacy decision.

1.6 "Controller", "processor", "data subject", "personal data", "personal data breach" and "processing" have the meanings given in Data Protection Law.

2. Roles

2.1 For Customer Personal Data, the Customer is the controller and EpassCard is the processor.

2.2 EpassCard is a controller for the data it needs to run its own business, such as account sign-in, billing, support and security logs. Its Privacy Policy at https://www.epasscard.com/privacy-policy/ covers that data.

3. Processing on instructions

3.1 EpassCard processes Customer Personal Data only on the Customer's documented instructions. These are the Terms, this DPA and the Customer's use and configuration of the Services.

3.2 If applicable law requires other processing, EpassCard will inform the Customer before processing, unless that law prohibits it.

3.3 EpassCard will promptly inform the Customer if, in its opinion, an instruction infringes Data Protection Law.

3.4 The Customer is responsible for having a lawful basis for the processing and for giving data subjects the information Data Protection Law requires.

4. Confidentiality

EpassCard ensures that every person it authorises to process Customer Personal Data is bound by an appropriate duty of confidentiality.

5. Security

5.1 EpassCard implements and maintains the technical and organisational measures described in Annex 2, in line with Article 32 UK GDPR.

5.2 EpassCard may update these measures over time, provided the overall level of protection is not reduced.

6. Sub-processors

6.1 The Customer gives EpassCard general written authorisation to engage Sub-processors. Annex 3 lists the Sub-processors in use on the date of this DPA.

6.2 EpassCard will notify the Customer by email at least 30 days before it adds or replaces a Sub-processor. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection in good faith, the Customer may terminate the affected Services and receive a pro-rata refund of any prepaid fees for them.

6.3 EpassCard imposes on each Sub-processor written data protection obligations that offer at least the same level of protection as this DPA. EpassCard remains liable to the Customer for the performance of its Sub-processors.

7. Data subject requests

7.1 The Services allow the Customer to access, correct, export and delete the pass data of its card holders.

7.2 If EpassCard receives a request from a data subject about Customer Personal Data, it will forward the request to the Customer without undue delay and will not respond to it unless the Customer instructs it to.

7.3 EpassCard will provide reasonable assistance with requests that the Customer cannot handle through the Services.

8. Personal data breaches

8.1 EpassCard will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data.

8.2 The notice will describe, as far as then known, the nature of the breach, the categories and approximate number of data subjects and records concerned, its likely consequences, and the measures taken or proposed. EpassCard will provide further information as it becomes available and will cooperate with the Customer's response.

9. Impact assessments and consultation

EpassCard will provide reasonable assistance to the Customer with data protection impact assessments and any prior consultation with the Information Commissioner's Office or another supervisory authority relating to the Services.

10. Deletion and return

10.1 During the term, the Customer can export and delete its pass data within the Services.

10.2 On termination of the Services, EpassCard will delete Customer Personal Data within 30 days, unless applicable law requires it to be kept. Copies held in backups are deleted in the normal backup cycle and remain protected by this DPA until then.

11. Information and audits

11.1 EpassCard will make available all information reasonably necessary to demonstrate compliance with Article 28 UK GDPR, including written responses to reasonable security questionnaires.

11.2 Where that information is not sufficient, or a supervisory authority requires it, the Customer may conduct an audit itself or through an independent auditor bound by confidentiality, on 30 days' written notice, no more than once a year (except following a personal data breach), during business hours and at the Customer's cost.

12. International transfers

12.1 EpassCard LLC is established in the United States, and its engineering and support team operates from Bangladesh. Customer Personal Data is processed in the locations listed in Annex 3.

12.2 **UK transfers.** For Restricted Transfers from the UK, the parties enter into the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under section 119A of the Data Protection Act 2018 (version B1.0, in force 21 March 2022) (the "**UK Addendum**"), which is incorporated into this DPA. For its Tables: Table 1, the parties are the Customer (exporter) and EpassCard LLC (importer) with the details in the signature block; Table 2, the Approved EU SCCs in clause 12.3, Module Two, with the options selected there; Table 3, Annexes 1, 2 and 3 of this DPA; Table 4, neither party may end the UK Addendum under its Section 19.

12.3 **EU transfers.** For Restricted Transfers from the EEA, the parties enter into the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), incorporated by reference. Clause 7 applies. Under Clause 9, option 2 (general written authorisation) applies, with the notice period in clause 6.2. The optional wording in Clause 11 does not apply. Under Clause 17, option 1 applies with the law of Ireland, and under Clause 18 the courts of Ireland are chosen. Annexes I, II and III of the SCCs are Annexes 1, 2 and 3 of this DPA.

12.4 **Onward transfers.** Where a Sub-processor outside the UK or EEA processes Customer Personal Data, EpassCard puts in place the UK Addendum and the EU Standard Contractual Clauses (Module Three), or another transfer mechanism recognised by Data Protection Law.

12.5 EpassCard will provide reasonable information to support the Customer's transfer risk assessment.

13. Liability, term and governing law

13.1 Each party's liability under this DPA is subject to the limitations in the Terms, except where Data Protection Law does not permit such a limitation.

13.2 This DPA remains in force for as long as EpassCard processes Customer Personal Data on behalf of the Customer.

13.3 For a Customer established in the UK, this DPA is governed by the laws of England and Wales, and the courts of England and Wales have jurisdiction. The UK Addendum and the EU Standard Contractual Clauses are governed by their own governing law and jurisdiction clauses.

Annex 1: Details of processing

Subject matter	Hosting the Customer's pass templates, and issuing, delivering and updating digital wallet passes to the Customer's card holders.
Duration	The term of the Customer's subscription, then until deletion under clause 10.
Nature and purpose	Storage, structuring, display, transmission and deletion of data so the Customer can create passes, send them by link, email, SMS or QR code, add them to Apple Wallet and Google Wallet, update them (points, stamps, balances, expiry and notifications) and scan them.
Data subjects	(a) The Customer's card holders, such as members, customers, players, staff and guests. (b) The Customer's team members who use the account.
Categories of personal data	Data the Customer chooses to place on or collect for a pass, typically name, email address, phone number, membership or customer number, photo and date of birth (if the Customer adds them), points, stamps, balance and tier, pass serial number and status, scan and redemption history, and form responses. Technical data: device push tokens used by Apple Wallet and Google Wallet for updates, and IP address and user agent when a pass is downloaded. For team members: name, email address, role and activity log.
Special category data	None is required. The Customer will not place special category or criminal offence data on passes unless it has a lawful basis and has informed EpassCard in writing.
Frequency	Continuous, for the duration of the Services.
Retention	As set by the Customer during the term; deleted under clause 10 on termination.
Competent supervisory authority	For UK transfers, the Information Commissioner's Office. For EU transfers, the authority under Clause 13 of the EU Standard Contractual Clauses.

Annex 2: Technical and organisational security measures

Area	Measure
Encryption in transit	All EpassCard websites, apps and the API are served over HTTPS only, with HTTP Strict Transport Security across all subdomains and TLS 1.3 supported.

Encryption of stored data	Account email addresses are stored encrypted with AES-256-GCM, with managed key rotation.
Passwords	Stored only as one-way bcrypt hashes.
Authentication	Email verification on sign-up by one-time code. Optional 2-step verification by one-time code, valid for 5 minutes.
Access control	Role-based team permissions within each customer account, and an audit log of changes. EpassCard staff access Customer Personal Data only where needed to run, support or fix the Services, under a duty of confidentiality.
Network protection	All traffic passes through Cloudflare for TLS termination and protection against network attacks.
Payments	Card payments are taken on Stripe Checkout (PCI DSS Service Provider Level 1). EpassCard does not store card numbers.
Logging	API logs mask keys and tokens. Application errors are monitored so faults can be fixed promptly.
Change management	Code changes pass automated tests, including an authentication test suite, before deployment to production.
Deletion	Customers can delete passes and their account themselves within the Services.

Annex 3: Sub-processors

Sub-processor	Purpose	Data	Location
DigitalOcean, LLC	Hosts the application, API, database and job queues	All Customer Personal Data	United States
Cloudflare, Inc.	Network security, and storage of uploaded files such as logos, banners and card holder photos	IP address, request data, uploaded files	Global network, United States
Apple Inc.	Apple Push Notification service, to update passes in Apple Wallet	Device push tokens, pass serial numbers	United States
Google LLC	Google Wallet API and Firebase, to issue and update passes and send app notifications	Pass content, object IDs, device tokens	United States
Twilio Inc.	Delivery of passes by SMS, where the Customer uses SMS	Phone number, message text	United States
Functional Software, Inc. (Sentry)	Application error monitoring	Technical data, which may include a user ID	United States
Crisp IM SAS	In-app support chat	Team member name, email address, chat messages	European Union
WebCartisan LLC	Engineering and customer support	Customer Personal Data, only as needed to support or fix the Services	Bangladesh

Where the Customer connects its own email provider or SMS account in the Services, that provider acts on the Customer's behalf and is not an EpassCard Sub-processor.

Signatures

	Customer (Controller)	EpassCard LLC (Processor)
Organisation		EpassCard LLC
Address		1209 Mountain Road Pl NE, Ste R, Albuquerque, NM 87110, United States
Data protection contact		privacy@epasscard.com
Name and role		Mahmudul Hasan, Founder and CEO
Signature		
Date		19 November 2026