

Privacy Policy

Park Pass Travel LLC

Last Updated September 21 2026

This Privacy Policy explains how Park Pass Travel LLC ("Park Pass," "Company," "we," "us," or "our"), collects, uses, discloses, and retains personal information and describes the privacy choices and rights that may be available to you. It consolidates our general United States privacy disclosures and our California disclosures into one policy.

Please read this Policy before using our Services or providing personal information. If you do not agree with our practices, do not provide personal information or use the Services.

Scope at a glance

This Policy covers our website, online store, travel-planning and booking interactions, accounts, customer service, marketing communications, and any other service that links to this Policy. It does not control the independent privacy practices of travel suppliers, payment processors, social-media platforms, or other third parties.

1 Scope and Relationship to Other Notices

This Policy applies to www.parkpasstravel.com, related pages, features, applications, online and offline communications, products, travel-planning and booking services, and other services that link to it (collectively, the "Services"). It applies whether you interact with us as a visitor, customer, traveler, account holder, subscriber, or a person acting for another traveler.

Transaction-specific notices, consent requests, or supplier terms may provide additional information at the point of collection. Our Website Terms of Use, available at www.parkpasstravel.com/privacy, governs use of the Services. If a separate notice conflicts with this Policy, the more specific notice controls for the activity it covers.

This Policy does not apply to information processed solely in an employment or independent-contractor context, or to a third party's website, application, service, or independent processing. When we act only as a service provider or processor for another business, that business's privacy notice governs its decisions about personal information.

2 What Personal Information Means

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to an individual or household. Depending on applicable law, it may also be called "personal data."

Personal information does not include information lawfully made available from government records, information that applicable law treats as publicly available, or deidentified or aggregated information that cannot reasonably be linked to an individual or household. We may use deidentified or aggregated information for any lawful purpose and will maintain and use deidentified information without attempting to reidentify it, except as permitted by law to test our deidentification processes.

3 Personal Information We Collect

The personal information we collect depends on how you interact with us. The following table describes categories we may collect and the corresponding categories used by the California Consumer Privacy Act, as amended (the "CCPA"). It also serves as our notice at collection for California consumers. We do not necessarily collect every example listed.

Category	Examples	Purposes
Identifiers and contact information (CCPA A)	Name, alias, postal and email addresses, telephone number, account name, online identifiers, IP address, loyalty or customer number, and similar identifiers.	Create and administer accounts; communicate; provide quotes, bookings, products, and support; ship orders; authenticate users; secure the Services; prevent fraud; maintain records; and market with applicable choice.
Customer records and financial information (CCPA B)	Billing and shipping information, signatures, insurance information, payment details handled by payment processors, and traveler data. Government-issued identification or passport information may be collected when needed for a requested travel service.	Process payments; complete, service, and document transactions and travel arrangements; prevent fraud; provide support; meet supplier requirements; and comply with law.
Protected characteristics (CCPA C)	Age or date of birth, citizenship or nationality, disability or accessibility information, marital or family status, and other characteristics you provide when relevant to travel, accommodations, or a request.	Determine eligibility; arrange requested travel or accessibility services; meet supplier or legal requirements; and provide support. We do not use this information for unlawful discrimination.
Commercial information (CCPA D)	Products, services, trips, tickets, reservations, destinations, or content purchased, obtained, considered, saved, or requested; transaction history; preferences; refunds; and customer-service records.	Complete and support transactions; maintain records; personalize and improve Services; analyze demand and performance; prevent fraud; and market related offerings with applicable choice.
Biometric information (CCPA E)	Biometric identifiers or templates used to establish identity, if a feature or supplier requires them. Ordinary photographs are addressed under sensory information.	If collected, provide the requested feature, authenticate identity, prevent fraud, or meet supplier requirements.
Internet or network activity (CCPA F)	Browsing and search activity on the Services, clicks, page and advertisement interactions, referring URLs, access times, cookie or device identifiers, and email engagement.	Operate and secure the Services; remember settings; diagnose errors; measure performance; conduct analytics; detect fraud; personalize content; and support advertising where enabled.
Geolocation (CCPA G)	Approximate location inferred from IP address. Precise location only if you enable a feature that requires it.	Localize content; provide destination, itinerary, or location features; secure transactions; detect fraud; and provide requested services.
Sensory and submitted content (CCPA H)	Photographs, video, audio, reviews, messages, call or chat content, support communications, and other content you choose to submit.	Provide requested features and support; respond to inquiries; moderate content; maintain quality and security; resolve disputes; and use content as authorized by you.
Professional information (CCPA I)	Employer, business contact information, role, or professional affiliation when you contact us for business travel, partnerships, or another commercial purpose.	Manage business relationships, arrange business travel or services, communicate, and maintain records.
Education information (CCPA J)	Education records or student information, if voluntarily provided for a group, student, or educational travel request.	If collected, provide the requested service and meet related supplier requirements.
Inferences and preferences (CCPA K)	Travel, destination, attraction, product, content, and communication preferences inferred from interactions, purchases, surveys, or requests.	Personalize and improve Services; provide recommendations; conduct analytics; and market relevant offerings with applicable choice.
Sensitive personal information (CCPA L)	Account credentials; payment data; government identifiers needed for travel; precise geolocation if enabled; citizenship or immigration information; racial or ethnic origin, health or accessibility information, or sexual orientation if voluntarily provided and relevant to a request; and information about a known child traveler supplied by a parent or guardian.	Provide requested services; process transactions; authenticate users; maintain security; prevent fraud; comply with law; and meet travel-supplier requirements. See Section 4.

Collection during the preceding 12 months. We expect to have collected CCPA categories A, B, C, D, F, G, H, I, K, and L as described above.

4 Sensitive Personal Information

We collect sensitive personal information only when reasonably necessary for a disclosed purpose. Examples may include login credentials; payment information; a passport number or other government identifier required

for travel; precise geolocation that you choose to enable; health, accessibility, dietary, citizenship, or similar information needed to fulfill a request; and information about a child traveler that a parent or legal guardian provides.

We use and disclose sensitive personal information to provide requested goods and services; process and secure transactions; authenticate users; prevent, detect, and investigate fraud or security incidents; ensure physical safety; comply with legal obligations; and perform other purposes permitted without a right to limit under applicable law. We do not use or disclose sensitive personal information to infer characteristics about you unless we first provide any notice and right to limit required by law.

4.1 Travel Documents and Identity Information

Depending on the itinerary and supplier, we may collect a traveler's legal name, aliases, date of birth, gender marker, citizenship or nationality, country of residence, passport or other government identification details, visa and immigration information, Known Traveler Number, redress number, loyalty-program identifier, signature, and related documents. We collect these details only when reasonably necessary to quote, reserve, ticket, service, or document travel; verify identity; prevent fraud; satisfy a supplier or government requirement; or assist during a disruption or emergency.

4.2 Itinerary Companion and Emergency Information

We may collect destinations, dates, routes, accommodations, ticket and confirmation numbers, room or cabin preferences, travel companions, group affiliations, emergency contacts, and communications concerning changes, cancellations, incidents, refunds, or claims. An itinerary may reveal sensitive details about a person's location, associations, religion, health, or other characteristics. We use and disclose itinerary information only for the purposes described in this Policy and as directed or permitted by the traveler or booking organizer.

4.3 Health Accessibility Dietary and Consumer Health Data

At your request, we may process information about disability, mobility, medical conditions, medications, allergies, pregnancy, dietary or religious needs, service animals, vaccination or testing documentation, or emergency assistance. Some state laws define consumer health data broadly and may cover information that identifies a past, present, or future health condition, treatment, location, or attempt to obtain health-related services. Where those laws apply, we will provide any required supplemental notice and obtain consent required for collection, use, or sharing.

We do not sell consumer health data without the separate written authorization required by applicable law, and we do not use geofencing around health-care facilities to identify or collect consumer health data where prohibited.

4.4 Information About Other Travelers

If you provide personal information about a family member, travel companion, employee, group participant, emergency contact, or other person, you represent that you are authorized to provide it for the requested purpose. You should give that person access to this Policy and any transaction-specific notice. A group leader, employer, sponsor, or booking organizer may receive itinerary and servicing information for travelers within the group when reasonably necessary to manage the trip, subject to law and the parties' arrangements.

4.5 Payment Insurance and Claims Information

Payment processors may collect payment-card or bank information, billing details, authentication results, and transaction identifiers. We may receive limited payment information and records needed to reconcile charges, issue refunds, address chargebacks, prevent fraud, and maintain accounts. If you request travel insurance or assistance with a claim, we may process policy selections, beneficiaries, claim communications, incident details, and supporting documents and disclose them to the insurer, assistance provider, or claims administrator. Their separate privacy notices apply to their independent processing.

5 Sources of Personal Information

- Directly from you, including through accounts, orders, payment and booking requests, quote forms, traveler profiles, surveys, reviews, support requests, messages, and marketing sign-ups.
- From a person acting for you, such as a family member, travel companion, group organizer, employer, or authorized agent. If you give us another person's information, you represent that you are authorized to do so and to permit us to use it as described in this Policy.
- Automatically from browsers and devices through cookies, pixels, local storage, software development kits, server logs, and similar technologies.
- From travel suppliers and partners, such as airlines, lodging providers, cruise lines, tour operators, ticket issuers, transportation providers, attractions, travel insurers, and referral partners, in connection with quotes, bookings, itineraries, changes, refunds, or support.
- From vendors that support payment processing, fraud prevention, shipping, identity verification, analytics, advertising, communications, customer service, and information security.
- From public sources and social-media services when you make information public or interact with us through those services.
- From group leaders, employers, schools, sponsors, meeting planners, travel companions, parents or guardians, emergency contacts, and other persons arranging or supporting travel.
- From host agencies, travel consortia, global distribution systems, central reservation systems, booking and ticketing platforms, destination-management companies, travel-assistance providers, insurers, and claims administrators.
- From government agencies, border or security authorities, fraud-prevention networks, sanctions-screening sources, and emergency responders where permitted or required by law.

6 How We Collect Information Online

6.1 Cookies and Similar Technologies

We and authorized providers may use cookies, pixels, tags, local storage, software development kits, and similar technologies. Some are necessary to operate the Services, remember settings, maintain security, or complete transactions. Others help us understand use, improve performance, measure communications and campaigns, personalize content, or support advertising where enabled.

Your browser or device may allow you to block or delete cookies. Blocking necessary technologies can impair functionality. Where required, our consent or preference tool allows you to manage nonessential technologies: Our site allows the user to make an acceptance or rejection selection via a modal upon entering the site. Choices made through that tool generally apply to the browser and device used and may need to be renewed if cookies are deleted.

6.2 Analytics Advertising and Social Features

We may use analytics providers to measure how people use the Services. We may also permit advertising or social-media partners to collect information through the Services to measure ads, limit repetition, build or select audiences, or display advertising based on activity over time and across nonaffiliated websites or services. These practices may constitute targeted advertising, cross-context behavioral advertising, "sharing," or a "sale" under some state privacy laws even if no money changes hands. See Sections 10 and 13 for choices.

Third parties control their own technologies and may combine information collected through our Services with information from other sources. Their processing is governed by their privacy notices.

7 How We Use Personal Information

- provide, operate, maintain, personalize, and improve the Services, products, content, recommendations, travel planning, bookings, and customer support;
- create and administer accounts, traveler profiles, saved items, subscriptions, and preferences;
- prepare quotes and itineraries and process payments, orders, deliveries, reservations, confirmations, cancellations, credits, returns, and refunds;

- communicate about transactions, accounts, service changes, security, policies, questions, emergencies, and support;
- send marketing and measure engagement where permitted, and honor communication choices;
- conduct analytics, research, testing, quality assurance, and development;
- personalize content, recommendations, offers, and advertising where permitted;
- authenticate users; maintain security; detect, investigate, and prevent fraud, abuse, unauthorized access, and other unlawful activity;
- protect the rights, property, health, and safety of users, travelers, the public, Company, and others;
- comply with applicable law, supplier requirements, tax and accounting obligations, and valid legal process;
- enforce agreements, collect amounts owed, and establish, exercise, or defend legal claims; and
- carry out another purpose disclosed when information is collected or with your consent.
- verify traveler identity and eligibility; populate passenger manifests; support ticketing, check-in, border, security, visa, and entry requirements; and match traveler information to supplier records;
- manage schedule changes, disruptions, rebooking, emergency assistance, duty-of-care communications, special requests, insurance, claims, loyalty programs, and group travel;
- operate through host agencies, consortia, global distribution systems, central reservation systems, and other booking, ticketing, itinerary, and payment platforms; and

8 Automated Tools and Artificial Intelligence

We may use automated tools to support fraud detection, security, search, recommendations, itinerary assistance, customer service, translation, content moderation, or operational efficiency. These tools may process personal information subject to contractual, security, and access controls appropriate to the use.

We do not use automated decisionmaking technology to make a significant decision producing legal or similarly significant effects concerning a consumer unless we provide any required pre-use notice and access, opt-out, or appeal rights.

9 How We Disclose Personal Information

We may disclose personal information to the following recipients for the purposes described in this Policy:

- Service providers and contractors supporting hosting, cloud storage, software, payment processing, order fulfillment, shipping, identity verification, fraud prevention, cybersecurity, analytics, communications, marketing operations, document management, and customer service.
- Travel suppliers and travel partners as necessary to obtain quotes, make and service reservations, complete travel, coordinate itineraries, satisfy identification or accessibility needs, address emergencies, or handle changes, cancellations, disputes, and refunds.
- Advertising, analytics, and social-media partners, subject to the notice and opt-out rights described in this Policy.
- Affiliates and professional advisers, including attorneys, accountants, auditors, insurers, lenders, and consultants, for legitimate business, risk-management, compliance, and legal purposes.
- Government authorities, regulators, courts, law enforcement, counterparties, and other persons when required by law or reasonably necessary to respond to legal process, protect rights or safety, investigate misconduct, or enforce agreements.
- A buyer, investor, lender, successor, or other participant in an actual or proposed merger, acquisition, financing, reorganization, bankruptcy, sale, or transfer of all or part of our business or assets.
- Other recipients at your direction or with your consent.

Travel suppliers and other third parties may act as independent businesses for information they receive and determine how to use. Their privacy notices apply to their independent processing. We encourage you to review those notices before completing a transaction.

- Host agencies, travel consortia, global distribution systems, central reservation systems, booking and ticketing platforms, itinerary tools, destination-management companies, and group-travel coordinators that help arrange or service travel.

- Travel insurers, assistance companies, medical or security assistance providers, and claims administrators when you request coverage, assistance, or claim support.
- Embassies, consulates, customs, immigration, border, aviation-security, public-health, law-enforcement, and emergency authorities where required or reasonably necessary for travel, safety, or legal compliance.

A Travel Supplier or booking-system participant may receive personal information before a reservation is completed so that it can return availability, pricing, or eligibility information. Once a recipient independently determines how and why to process the information, its own privacy notice and applicable law govern that processing.

10 Sale Sharing and Targeted Advertising

We do not sell personal information for money. Certain disclosures to advertising, analytics, or social-media partners may be considered a "sale" of personal information, "sharing" for cross-context behavioral advertising, or targeted advertising under state privacy laws.

You may opt out of covered sale, sharing, or targeted advertising through www.parkpasstravel.com/privacy or by enabling a legally recognized universal opt-out mechanism, such as Global Privacy Control, in a supported browser. We process a signal as a request for the browser or device that sends it and, when we can associate it with your account, may apply it more broadly. We do not require you to create an account to opt out.

We do not knowingly sell or share the personal information of consumers under age 16 for cross-context behavioral advertising without the affirmative authorization required by law.

11 California Disclosure of Prior 12 Month Practices

The table below summarizes our expected collection and disclosure practices during the 12 months before this Policy's Last Updated date. It must be confirmed against Park Pass's actual data inventory before publication. "Business-purpose recipients" includes service providers, contractors, travel suppliers, and the other recipients described in Section 9. "Sale or sharing" has the broad CCPA meaning described in Section 10.

CCPA category	Collected	Disclosed for business purposes to	Sold or shared
A Identifiers	Yes	Service providers; travel suppliers; shippers; advisers; authorities; transaction parties	See Section 10
B Customer records	Yes	Payment and identity providers; travel suppliers; shippers; advisers; authorities	No expected
C Protected characteristics	Yes, when relevant	Travel suppliers; accessibility and support providers; authorities when required	No expected
D Commercial information	Yes	Service providers; travel suppliers; analytics providers; advisers; transaction parties	See Section 10
E Biometric information	N/A	If collected: identity or feature providers and relevant travel suppliers	No expected
F Internet or network activity	Yes	Hosting, security, analytics, advertising, communications, and social-media providers	See Section 10
G Geolocation	Yes, approximate; precise only if enabled	Hosting, security, feature, analytics, and travel providers	See Section 10
H Sensory information	Yes, if submitted	Customer-support, communications, content, security, and professional providers	No expected
I Professional information	Yes, if provided	Business-operations providers; travel suppliers; advisers	No expected
J Education information	N/A	If collected: service providers and travel suppliers	No expected
K Inferences	Yes	Analytics, personalization, marketing, and advertising providers	See Section 10
L Sensitive personal information	Yes, when needed	Payment, identity, security, and travel providers; authorities when required	No expected

12 Retention

We retain personal information only for as long as reasonably necessary and proportionate for the purposes described in this Policy. The period depends on the nature and sensitivity of the information, the amount and context of processing, the relationship or transaction involved, the risk of harm from unauthorized use, whether the purpose can be achieved another way, and legal, accounting, tax, fraud-prevention, supplier, dispute-resolution, and recordkeeping requirements.

In general, we retain account and relationship information while an account or customer relationship remains active; transaction, booking, tax, and payment records for the period required by law and reasonably needed for audits, chargebacks, disputes, and fraud prevention; marketing information until you opt out or it is no longer useful, subject to suppression records needed to honor your choice; and cookie or device data according to the relevant technology's duration and our security and analytics needs. We may retain deidentified information for longer.

We seek to limit retention of passport, visa, government-identifier, health, accessibility, dietary, precise-location, and child-traveler information to the period reasonably necessary for the booking, travel, servicing, safety, fraud-prevention, dispute, and legal purposes for which it was collected. A Travel Supplier, global distribution system, insurer, or government authority may retain its own copy under its separate requirements. We may retain a suppression record, audit trail, or transaction record without retaining the underlying sensitive document when reasonably feasible.

13 Your Choices

13.1 Account and Transaction Information

You may update certain account information through available account settings or by contacting us. You are responsible for keeping information accurate, particularly traveler names and details that must match travel documents. We may retain prior information when required for records, security, fraud prevention, or legal compliance.

13.2 Marketing Communications

You may unsubscribe from promotional emails through the link in the message, through available preferences, or by contacting privacy@parkpasstravel.com. We may continue to send non-marketing communications about transactions, accounts, security, support, and our legal relationship with you. Consent to marketing is not a condition of purchase.

13.3 Cookies Targeted Advertising and Universal Opt-Out Signals

Use www.parkpasstravel.com/privacy to manage available cookie and advertising choices. You may also use browser or device controls. Where applicable law requires, we honor recognized universal opt-out signals, including Global Privacy Control, as described in Section 10. Because these choices can be browser- and device-specific, you may need to set them on each browser and device.

13.4 Location Information

You can control precise location access through device permissions. If you withdraw permission, location-based features may not function, but we may continue to infer an approximate location from an IP address for security, localization, or analytics.

13.5 Traveler Profiles and Special Requests

You may ask us to update or remove information stored in a traveler profile, subject to transaction, security, legal, and supplier requirements. Removing passport, loyalty, accessibility, dietary, or other profile information may prevent us from applying it to future bookings. You should not send passport, payment, health, or other highly sensitive information through ordinary email or an unencrypted form when we provide a secure submission method.

14 U.S. State Privacy Rights

Depending on your state of residence, the law that applies to Park Pass, and applicable exceptions, you may have the right to:

- confirm whether we process your personal information and access or obtain a copy of it;
- request correction of inaccurate personal information;
- request deletion of personal information;
- obtain personal information you provided in a portable and, where technically feasible, readily usable format;
- obtain information about categories or specific pieces of personal information, sources, purposes, and categories of recipients;
- opt out of sale, targeted or cross-context behavioral advertising, or certain profiling or automated decisionmaking;
- limit certain uses or disclosures of sensitive personal information;
- withdraw consent where processing is based on consent;
- appeal our decision concerning a request; and
- receive equal service and pricing without unlawful discrimination for exercising a privacy right.

These rights are not absolute. We may deny or limit a request when an exception applies, such as when information is needed to complete a transaction, maintain security, comply with law, protect rights, or exercise or defend legal claims. We will explain a denial when required.

15 How to Exercise a Privacy Right

Submit a request using one of the following methods:

- Web form: www.parkpasstravel.com
- Email: privacy@parkpasstravel.com
- Privacy choices: www.parkpasstravel.com/privacy

Describe the right you wish to exercise and provide information reasonably necessary to locate relevant records. We will acknowledge and respond within the period required by applicable law. For California requests to know, delete, or correct, we generally acknowledge receipt within 10 business days and respond within 45 calendar days. We may extend the response period once by up to 45 additional days when reasonably necessary and will explain the extension. Requests to opt out of sale or sharing or to limit use of sensitive personal information will be processed as soon as feasible and no later than the period required by law.

We do not charge a fee unless permitted by law, such as when a request is manifestly unfounded, excessive, or repetitive. If we charge a fee or decline to act, we will explain the basis where required. Responses to access or portability requests will use a readily usable format when required.

16 Verification Authorized Agents and Appeals

16.1 Verification

We verify requests by matching information you provide with information in our records and may request additional information appropriate to the nature and sensitivity of the request. We use verification information only to verify identity or authority. If we cannot verify a request, we may deny it or provide a more limited response. We will never ask for a password through an unsolicited email or telephone call.

16.2 Authorized Agents

Where permitted, an authorized agent may submit a request for you. We may require proof that you authorized the agent, ask you to verify your identity directly, or ask you to confirm the authorization. These steps do not apply when the agent holds a valid power of attorney under applicable law. An agent may submit a request through the methods in Section 15 and should identify the request as an authorized-agent request.

16.3 Appeals

If we deny a request and your state provides a right to appeal, you may appeal by replying to our decision or emailing privacy@parkpasstravel.com with the subject line "Privacy Appeal." Explain why you believe the decision should be reconsidered. We will respond within the period required by applicable law and, where required, provide information about how to contact the appropriate regulator or attorney general.

17 Additional California Disclosures

If the CCPA applies to our processing, California residents have the rights described in Sections 14 through 16, including rights to know, access, delete, correct, and obtain information; to opt out of sale or sharing; to limit certain uses or disclosures of sensitive personal information; and to be free from unlawful discrimination. The categories of information, sources, purposes, retention criteria, and recipient categories are described in Sections 3 through 12.

We do not discriminate against a consumer for exercising a CCPA right. For example, we will not deny goods or services, charge a different price, provide a different quality, or retaliate against an employee or applicant because of a request, except as permitted by law. If we offer a financial incentive or price or service difference related to personal information, we will provide a separate notice explaining the material terms and value calculation and obtain any required opt-in consent.

California's "Shine the Light" law may permit certain residents to request information about disclosures of specified personal information to third parties for their own direct-marketing purposes. Submit a request to privacy@parkpasstravel.com with the subject line "California Shine the Light Request." We may satisfy this law by maintaining a policy not to disclose covered information for third parties' direct marketing without choice.

18 Nevada Residents

Nevada residents may submit a verified request directing us not to make a covered sale of certain personal information under Nevada law. Nevada defines a sale more narrowly than some other state laws. We do not currently sell covered information for monetary consideration as defined by Nevada law. You may submit a request to privacy@parkpasstravel.com.

19 Children and Teenagers

The Services are intended for a general audience and are not directed to children under age 13. A person must be at least 18 to create an account, make a purchase, complete a booking, subscribe to marketing, or otherwise enter into a transaction with us. Parents and legal guardians may use the Services to plan and purchase travel or other services for their children.

We do not knowingly collect personal information online directly from a child under age 13 without verifiable parental consent. A parent or legal guardian may provide information about a child traveler—such as name, age, date of birth, passport details, accessibility or dietary needs, and itinerary information—when reasonably necessary for a family purchase or travel arrangement. We treat that information as submitted by the adult, use it only as described in this Policy, and disclose it to relevant travel suppliers and service providers as needed to fulfill the request.

If we learn that a child under age 13 provided personal information directly to us without the required authorization, we will take reasonable steps to delete it. A parent or guardian who believes a child provided information directly may contact privacy@parkpasstravel.com to request review, correction, or deletion and to refuse further collection or use. We may take reasonable steps to verify the requester's identity and relationship to the child.

If we later offer a feature directed to children under age 13 or knowingly collect personal information online directly from them, we will provide any required direct parental notice, obtain verifiable parental consent, limit collection to what is reasonably necessary, provide parental access and deletion rights, and retain the information only as long as needed. As stated in Section 10, we do not knowingly sell or share personal information of consumers under age 16 without required affirmative authorization.

20 Security

We use reasonable administrative, technical, and physical safeguards designed to protect personal information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Safeguards may include access controls, vendor management, encryption where appropriate, monitoring, incident-response procedures, and workforce training. No method of transmission or storage is completely secure, and we cannot guarantee absolute security.

You are responsible for maintaining the confidentiality of account credentials and for promptly notifying us of suspected unauthorized access. Email and ordinary web forms may not be appropriate for highly sensitive information; provide passport, payment, health, or similar data only through the secure method we designate.

We seek to minimize access to highly sensitive travel information and may use designated portals, tokenized payment services, role-based access, deletion schedules, or other safeguards appropriate to the information and risk. Do not send a full payment-card number, passport image, medical record, or authentication credential through ordinary email unless we specifically instruct you to use a protected method. If you believe sensitive information was sent insecurely or to the wrong recipient, contact us promptly.

21 International Processing

Park Pass is based in the United States. We and recipients described in this Policy may process personal information in the United States and other countries where travel suppliers or service providers operate. Privacy laws in those locations may differ from those where you live. We use appropriate measures required by applicable law for covered transfers. This Policy is directed to United States consumers unless a separate regional notice states otherwise.

International travel frequently requires disclosure of personal information to recipients located at the destination, in transit countries, or where a carrier, booking platform, host agency, or support provider operates. Those recipients may include private companies and government authorities, and local law may permit access or uses different from United States law. When a transfer is necessary to perform a requested booking or provide assistance, declining the transfer may prevent us from completing the service.

Where applicable law requires a transfer mechanism, contractual protection, consent, or other safeguard for our transfer, we will use the required measure. These protections do not change the independent obligations or practices of a Travel Supplier or authority that receives information directly for its own purposes.

22 Third Party Links and Services

The Services may link to or integrate with travel suppliers, payment processors, social-media platforms, advertisers, maps, or other third parties. We do not control and are not responsible for their independent privacy, security, content, or data practices. A link or integration does not imply endorsement. Review the third party's privacy notice before providing information.

23 Changes to This Policy

We may update this Policy to reflect changes in our practices, Services, or law. We will post the updated Policy and revise the Last Updated date. If required, we will provide additional notice or obtain consent before applying a material change to personal information previously collected. Prior versions may be requested through the contact information below.

24 Accessibility and Contact Information

This Policy is available in alternative formats upon request. To ask a question, request accessibility assistance, or exercise a privacy right, contact:

Park Pass Travel LLC d/b/a Park Pass International

Web form: www.parkpasstravel.com

- Email: privacy@parkpasstravel.com
- Privacy choices: www.parkpasstravel.com/privacy

25 Travel Materials Controls

Notwithstanding anything to the contrary set forth herein, in the event of any conflict between these Terms and any invoice, agreement, or other information provided directly to you by Company in connection with any travel or other purchase (collectively, "Travel Materials"), the Travel Materials shall govern and control.