TRAVEL CODE PRIVACY POLICY

Travel Code, Inc. 77 SE 5th Street, Suite 2805, Miami, Florida 33131, United States EIN 88-3712471 · IATA/ARC 10626195 · Florida Seller of Travel Reg. No. ST44595

---

1. ABOUT THIS POLICY

This policy explains how Travel Code, Inc. ("Travel Code", "we", "us") collects, uses, shares, and protects personal information.

Travel Code provides corporate travel management, expense management, and corporate payment card services to business customers. Most of the personal information we handle belongs to the **personnel of our business customers** — travellers, expense submitters, approvers, administrators, and cardholders.

This policy covers:

- our website, web application, and mobile applications;
- the services we provide to business customers; and
- our marketing, events, and business communications.

It does not cover third-party websites or services, or the separate privacy practices of our banking and card partners, which are described in their own notices.

---

2. OUR ROLE

Our role differs depending on whose information it is and why we hold it. This distinction matters because it determines who you should contact about your rights.

2.1 Where we act on behalf of a business customer (processor / service provider)

When we process personal information about a business customer's personnel in order to deliver travel booking, expense management, and related platform services, we act as a **processor** (a "service provider" or "contractor" under US state privacy laws) **on the documented instructions of that customer**, which is the controller.

If you are an employee, contractor, or authorized user of one of our business customers and you want to exercise rights over information processed in that capacity, **please contact your employer or account administrator first**. We will support them in responding, and we will refer requests we receive directly to them where appropriate.

2.2 Where we act for ourselves (controller)

We act as a **controller**, determining our own purposes and means, when we:

- operate our website and marketing, and communicate with prospective customers;
- verify identity and screen for sanctions, fraud, anti-money-laundering, and credit risk in connection with onboarding, including where we transmit information to our card partners;
- act as merchant of record for travel we sell, and maintain the resulting financial and transaction records;
- secure, monitor, and improve our platform; and
- meet our own legal, regulatory, tax, and recordkeeping obligations.

Our relationship with each business customer is governed by a Data Processing Addendum which sets out these roles in detail.

---

3. INFORMATION WE COLLECT

3.1 Information provided to us

- **Business contact and account information** — name, work email, phone, employer, job title, role and permissions, authentication credentials.
- **Traveller information** — name as it appears on travel documents, date of birth, gender where a supplier requires it, passport or national ID details, visa details, frequent traveller and loyalty numbers, seat and room preferences, and emergency contact details.
- **Expense information** — receipts and invoices and the data extracted from them, merchant names, amounts, dates, categories, descriptions, mileage, and per diem claims.
- **Financial and payment information** — billing details, bank account details for reimbursement, and information required by our card partners for onboarding.
- **Identity verification information** — for company representatives, beneficial owners, and control persons, including government-issued identifiers and identity documents, collected in connection with know-your-business and anti-money-laundering obligations.
- **Communications** — correspondence with our support, sales, and account teams, and, where permitted by law and with notice, recordings or transcripts of support calls.

3.2 Information collected automatically

Device and browser information, IP address, approximate location inferred from IP address, pages and features used, timestamps, referring pages, diagnostic and error data, and information collected through cookies and similar technologies. See our Cookie Policy.

3.3 Information from other sources

- **Travel suppliers and distribution partners** — airlines, hotels, rail and ground operators, and the global distribution systems we use, providing booking, ticketing, and disruption information.
- **Card partners** — our card program manager and the issuing bank, providing onboarding status, card and account status, and transaction data.
- **Financial account connections** — where a customer connects payment cards or financial accounts it holds at other institutions, we receive transaction data through a financial data aggregation provider. We do not receive or store online banking credentials.

- **Identity, sanctions, fraud, and credit reference providers.**
- **Publicly available sources** — company registries and similar sources, for due diligence and business development.

---

4. SENSITIVE INFORMATION

Some information we handle is treated as sensitive under applicable law:

- government-issued identifiers, passport and identity document details;
- financial account and payment card information;
- account access credentials;
- health-related information, where a traveller supplies accessibility, dietary, or medical requirements, or where a submitted receipt relates to a pharmacy or medical service.

We use sensitive information only to provide and operate the services, to process bookings and transactions, to detect and prevent fraud and security incidents, and to meet legal obligations. **We do not use or disclose sensitive information for purposes that would require offering a right to limit under applicable US state law, and we do not use it for advertising or profiling.**

Where a business customer's personnel submit receipts, those receipts may incidentally contain information beyond the transaction. We process such information only as part of the receipt and only to provide the services.

---

5. HOW WE USE PERSONAL INFORMATION

We use personal information to:

- provide travel booking, servicing, and traveller support, and to transmit the information suppliers require to complete a booking;
- provide expense capture, categorization, policy evaluation, per diem calculation, approval workflow, and reporting;
- enable customers to apply for and administer corporate cards issued by our banking partner, and to display card and account information in our platform;
- enable customers to connect payment cards and financial accounts they hold and view the resulting transaction data;
- process payments, invoices, reimbursement instructions, and rewards;
- provide duty-of-care and traveller-location features that our customers enable;
- verify identity and assess risk, including sanctions, fraud, anti-money-laundering, and credit checks;
- provide support and communicate about accounts, transactions, and service changes;
- secure, monitor, troubleshoot, and improve the platform;
- market our services to business contacts, subject to applicable law; and
- comply with legal, regulatory, tax, and recordkeeping obligations, and establish or defend legal claims.

5.1 Legal bases (for individuals in the EEA, UK, and Switzerland)

Where we act as a controller, we rely on: **performance of a contract**; **legitimate interests** in operating, securing, and improving our business and in business-to-business marketing; **legal obligation**, in particular for financial, tax, sanctions, and anti-money-laundering requirements; and **consent**, where required, for example for certain cookies or for special-category data such as accessibility requirements. Where we act as a processor, the legal basis is determined by our business customer.

---

6. ARTIFICIAL INTELLIGENCE

We use artificial intelligence to read and classify receipts, suggest expense categorization and policy outcomes, answer questions about data already in the platform, and assist with support and workflows.

- AI-generated output is **assistive and subject to human review**. It does not by itself determine an outcome.
- **No AI feature completes a financial operation autonomously.** Every automated financial workflow requires human confirmation before execution.
- To provide these features we transmit relevant data to AI model providers acting as our sub-processors. This may include receipt images and extracted content, merchant names, amounts, expense descriptions, traveller names, trip context, and the content of queries.
- **We contract with these providers on terms that do not permit your data to be used to train, retrain, or improve their models**, and we operate these services in a zero-data-retention configuration, under which the provider does not retain the content of requests or responses after the request is served.

---

7. WHO WE SHARE INFORMATION WITH

- **Our business customers.** Where you are a customer's personnel, we make information available to that customer, including to its administrators, finance team, and approvers, as its own policies determine.
- **Travel suppliers and distribution partners** — airlines, hotels, rail and ground operators, and global distribution systems, to make and service bookings.
- **Card program partners** — our card program manager and the issuing bank, for onboarding, card issuance, transaction processing, and regulatory compliance. **Cards are issued by Coastal Community Bank, Member FDIC, pursuant to a license from Visa U.S.A. Inc. Travel Code is a financial technology company, not a bank, and does not hold customer funds.** Those partners act as independent controllers for the financial services they provide, under their own privacy notices.
- **Financial data aggregation provider**, where a customer connects accounts held elsewhere.
- **Payment processors and reimbursement providers**, to collect amounts due and to execute reimbursement instructions given by a customer.
- **Service providers** — cloud hosting, email delivery, analytics, security monitoring, customer support tooling, AI model providers, and compliance tooling — who process on our behalf under contract.

- **Identity, sanctions, fraud, and credit reference providers.**
- **Professional advisers, auditors, and insurers.**
- **Authorities** — regulators, law enforcement, and courts, where required by law or legal process, and where necessary to protect rights, property, or safety.
- **Corporate transactions** — in connection with a merger, acquisition, financing, or sale of assets, subject to confidentiality protections.

A current list of our sub-processors is available at **trust.travel-code.com**. Business customers receive advance notice of changes as provided in their Data Processing Addendum.

We do not sell personal information.

Sharing for advertising. We use analytics and advertising technologies, and we work with advertising partners to show our ads on other websites and platforms. This may involve those partners collecting information about your interaction with our website through cookies and similar technologies. Under California law and some other state laws, this may be considered **"sharing"** for cross-context behavioural advertising.

The categories that may be shared are identifiers such as name, email address, IP address and device identifiers, internet and network activity information, and inferences drawn from them. They are shared with advertising networks, analytics providers, and marketing partners.

You may opt out of this sharing by using the "Do Not Sell or Share My Personal Information" link on our website, by adjusting your preferences in our cookie consent tool, or by sending a Global Privacy Control signal, which we honour. You may also contact us using section 14.

---

8. INTERNATIONAL TRANSFERS

We are based in the United States. Our primary infrastructure is hosted in the European Union (Amazon Web Services, Stockholm region). Information may be accessed from, transferred to, and processed in, the United States and other countries where we or our providers operate.

8.1 Data Privacy Framework

Travel Code, Inc. complies with the **EU-U.S. Data Privacy Framework**, the **UK Extension to the EU-U.S. Data Privacy Framework**, and the **Swiss-U.S. Data Privacy Framework** as administered by the U.S. Department of Commerce, in respect of personal data received from the European Union, the United Kingdom and Gibraltar, and Switzerland.

We have certified that we adhere to the **Data Privacy Framework Principles**. Where there is any conflict between this policy and the Principles, the Principles govern. To view our certification, see **https://www.dataprivacyframework.gov/list**.

Onward transfer liability. We remain **responsible and liable under the Principles** if a third party we engage to process personal data on our behalf does so in a manner inconsistent with the Principles, unless we prove we are not responsible for the event giving rise to the damage.

Regulatory authority. We are subject to the investigatory and enforcement powers of the **U.S. Federal Trade Commission**.

Lawful requests. We may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Independent recourse. If you have a complaint about our handling of personal data covered by the Data Privacy Framework, contact us first using the details in section 14. We will respond within **45 days**. If your complaint is not resolved, you may refer it, **free of charge to you**, to our independent recourse mechanism, **JAMS**, at https://www.jamsadr.com/DPF-Dispute-Resolution.

Binding arbitration. In certain circumstances, and where other avenues have not resolved your complaint, you may be able to invoke **binding arbitration** under Annex I to the Data Privacy Framework Principles.

8.2 Other transfer mechanisms

Where the Data Privacy Framework does not apply, or where a customer requires it, we rely on the **European Commission's Standard Contractual Clauses** and, for the United Kingdom, the **UK International Data Transfer Addendum**, together with any supplementary measures required.

---

9. RETENTION

We keep personal information only as long as necessary for the purposes described in this policy or as required by law.

We do not apply one retention period to everything. We determine the appropriate period based on the amount, nature, and sensitivity of the information, the risk of harm from unauthorized use or disclosure, whether the purpose can be achieved by other means, applicable legal, tax, and regulatory requirements, requirements imposed by our banking, card, and travel partners, and applicable limitation periods. **Actual retention periods therefore vary.**

In general: account and traveller data is kept for the life of the account; booking, expense, card, invoice, and rewards records are kept for the period required by financial, tax, and audit recordkeeping obligations; identity verification and anti-money-laundering records are kept for the period those obligations require after the relationship ends; support communications, security logs, and analytics data are kept for the period needed for their purpose. Where a record serves more than one purpose, the longest applicable period governs.

Information subject to a legal hold is preserved until the hold is lifted.

When a business customer's relationship with us ends, that customer may export its data for **90 days**, after which we delete it from active systems within **30 days**, except for records we are required to keep, backups awaiting overwrite in the ordinary cycle, data under legal hold, and de-identified data. Full detail is in our Data Retention Policy.

Our retention obligations may require us to keep information after you are no longer an authorized user or after your employer's account has closed, and may in some cases prevent us from deleting information when you ask us to.

10. SECURITY

We maintain a written information security programme with administrative, technical, and physical safeguards, including access controls, encryption in transit and at rest, logging and monitoring, and regular risk assessment and vulnerability management. Details of our security posture and certifications are available at trust.travel-code.com.

No system is completely secure. You are responsible for keeping your account credentials confidential. If we become aware of a security incident affecting personal information, we will investigate, mitigate, and notify affected parties and authorities as required by law.

---

11. YOUR RIGHTS — UNITED STATES

Depending on your state of residence, you may have the right to:

- **know** what personal information we collect, use, and disclose;
- **access** a copy of your personal information;
- **correct** inaccurate personal information;
- **delete** personal information we hold about you;
- **opt out** of the sale or sharing of personal information for cross-context behavioural advertising, and of profiling with legal or similarly significant effects;
- **limit** the use of sensitive personal information; and
- **not be discriminated against** for exercising your rights.

We do not sell personal information and we do not use sensitive personal information for purposes that trigger a right to limit.

To exercise a right, contact us using section 14. We will verify your identity before responding, and will respond within the time required by law — **45 days** under California law, subject to permitted extension. You may use an authorized agent, with proof of authority.

Appeals. If we decline your request, you may appeal by writing to privacy@travel-code.com with "Appeal" in the subject line. We will respond within the period required by your state's law. If your appeal is denied, you may contact your state Attorney General.

Important. Where we process information on behalf of a business customer, we act as a service provider and will direct your request to that customer, who is the appropriate party to respond.

---

12. YOUR RIGHTS — EEA, UK AND SWITZERLAND

Where we act as a controller, you may have the right to access, correct, erase, restrict, or object to processing, to data portability, and to withdraw consent where processing is based on consent. You may lodge a complaint with your supervisory authority, or with the Information Commissioner's Office in the United Kingdom or the Federal Data Protection and Information Commissioner in Switzerland.

Where we act as a processor for a business customer, please direct your request to that customer.

---

13. CHILDREN

Our services are provided to businesses and are not directed to children, and we do not market to children.

We may, however, process a child's information where an adult books family travel through our platform and supplies the details a supplier requires, such as a child's name and travel document details. In that case we process the information on the instruction of the adult booker or the business customer, solely to complete and service the booking.

We do not knowingly collect personal information directly from children, and we do not sell or share the personal information of individuals under 16. If you believe a child has provided us with information directly, contact us and we will delete it.

---

14. CONTACT

Travel Code, Inc. Attn: Privacy 77 SE 5th Street, Suite 2805, Miami, Florida 33131, United States Email: **privacy@travel-code.com** General: hello@travel-code.com · Phone: +1 646 722 8331

If you need this policy in an alternative accessible format, contact us and we will make reasonable efforts to accommodate.

---

15. CHANGES

We may update this policy. We will change the effective date above and, where changes are material and we have a relationship with you, we will provide notice through the services or by email. Where we do not, we will post the updated policy on our website.