SCHEDULE E — HR SYSTEM INTEGRATION & EMPLOYEE DATA

Version 1.0

This Schedule E forms part of the Travel Code Master Platform Agreement and applies when the Customer connects a human-resources information system (an "**HR System**") to the Travel Code Platform. Capitalized terms not defined here have the meaning given in the Master Agreement and the Data Processing Addendum ("**DPA**").

---

1. WHAT THE INTEGRATION DOES

1.1 Purposes. The integration is used only for the following purposes (the "**Integration Purposes**"):

(i) creating, updating and archiving employee accounts; (ii) placing employees in the correct company, department and cost center; (iii) routing trip and expense approvals to the employee's manager and, while the manager is absent, to their delegate; (iv) issuing tickets and carrying out visa and entry checks; (v) duty of care: locating and contacting travellers during disruptions and emergencies; and (vi) where the Customer switches it on, sending trips and expenses to the HR System's expense module.

Travel Code does not use data received through the integration for any other purpose, including marketing, profiling or product improvement, except as section 8 allows.

1.2 What it does automatically. Once activated, the integration:

(a) creates a Platform user for each employee of the HR System who is employed or about to start, in the company the Customer has mapped to that employee's legal entity or chosen for that employee; (b) updates the data listed in section 3 when it changes in the HR System; (c) archives the Platform user of an employee whom the HR System reports as no longer employed, and restores them if the HR System reports them employed again; and (d) places employees in departments and cost centers as recorded in the HR System.

1.3 Safeguards. Before the first run, and at any time afterwards, the Customer can see a preview of every change the integration would make, and a list of the employees it could not place, with the reason. The Customer may add such an employee with a company or email of its choosing, or exclude any employee from the integration. The integration never archives an employee only because the employee is missing from an HR System response, and it holds back unusually large numbers of archives until the Customer confirms them.

1.4 Timing. The integration reconciles all data at least once a day. Where the HR System supports it and the Customer's credential allows it, changes are also received in near real time.

1.5 The HR System stays the Customer's. The Customer's agreement with the provider of its HR System is between the Customer and that provider. Travel Code is not a party to it and is not responsible for the availability or accuracy of the HR System. The HR System provider is not a sub-processor of Travel Code.

---

2. CONNECTION AND CREDENTIALS

2.1 Access the Customer grants. The Customer connects the integration by giving Travel Code an access key or other credential issued by its HR System. The Customer chooses, in its HR System, which data that credential can read, and should give it only the scopes section 3 needs.

2.2 Read-only by default. Travel Code writes to the HR System only for a feature the Customer has separately switched on in the Platform, and only the data that feature lists before it is switched on. For the expense feature this is the employee identifier, trip and expense dates, merchant, amount, currency, category, cost center and, where the Customer selects it, the receipt image. Data written to the HR System is then the Customer's responsibility under its agreement with the HR System provider. The Customer may switch write-back off at any time without affecting the rest of the integration.

2.3 Security of credentials. Travel Code stores credentials encrypted, never shows them back in the Platform, and uses them only for this integration. The Customer may revoke a credential in its HR System at any time; the integration then stops.

---

3. DATA TRAVEL CODE RECEIVES AND WHY

3.1 Data categories. Subject to what the Customer's credential can read, Travel Code receives:

Data	Why the Platform needs it	What does not work without it
Employee identifier, name, work email	to create and recognise each employee's account	employees cannot sign in or be found
Personal email and personal phone, only where no work contact exists	to reach the employee during a disruption, and as sign-in email where the Customer chooses so	the employee may not be reachable
Employment status, start and end dates	to give and remove access at the right time	leavers keep access to company travel
Company / legal entity, establishment, department	to place employees in the right company and department	bookings and invoices go to the wrong company
Manager's identifier and name	only to route approvals and show the approval chain	trips cannot be sent to the right approver
Cost center, project and similar allocation values	to charge trips and expenses correctly	spend cannot be allocated in reports and invoices
Date of birth, sex, nationality, unless the Customer switches this off in the integration settings (then each traveller enters them before their first flight)	**required by airlines and other carriers to issue tickets**, and for visa and entry checks	airline tickets cannot be issued for the employee

Data	Why the Platform needs it	What does not work without it
Work phone number	disruption alerts, duty of care, 24/7 agent contact	the employee cannot be reached during a disruption
Absence dates and an absent/present indicator only, never the type or reason of the absence	forwarding approvals while an approver is absent; not sending travel alerts or booking prompts to someone on leave	approvals wait for an absent approver
Assigned work location (establishment, office address or remote-work country), not real-time or device location	duty of care (identifying employees at a site affected by an incident) and travel-policy rules by home location	travellers cannot be located in an emergency
Organisational reference data (job titles, categories, grades)	travel-policy rules by role or grade	role-based policy rules cannot apply

3.2 No reduced mode. The data in section 3.1 is what the Platform needs to perform the Services. Travel Code does not offer an integration that withholds it, because the Platform could not book travel for the employees concerned.

3.3 Data Travel Code never keeps. Travel Code keeps only the fields listed in section 3.1 (an allow-list). Any other field the HR System returns is discarded on receipt and is not stored, including: health data (including sickness, medical examinations and disability), the type or reason of any absence (for example sick, maternity, parental or religious leave), religious belief, trade-union membership, social-security and national-insurance numbers, salary and payroll data, tax data, marital status and data about family members. Bank-account details are received only if the Customer switches on employee reimbursements, and are then stored encrypted.

3.4 Traveller-entered data comes first. Where an employee has entered their own date of birth, sex, nationality, phone number, passport or loyalty details in the Platform, the integration does not overwrite them, because the employee's travel document is the reference airlines use.

3.5 Minimisation. Before the first run the Customer chooses which companies and employees the integration covers, and Travel Code reads only the categories in section 3.1.

---

4. ROLES AND THE CUSTOMER'S RESPONSIBILITIES

4.1 Roles. For employee data received through the integration, the Customer is the controller and Travel Code is its processor under the DPA. This Schedule E, together with the Customer's settings in the Platform, is the Customer's documented instruction for the purposes of Article 28(3)(a) GDPR. Where Travel Code passes traveller data to carriers and other travel suppliers to complete a booking, those suppliers act as independent controllers, and where Travel Code acts as merchant of record it processes booking records as a controller, as described in the Privacy Policy.

4.2 The Customer confirms that:

(a) it has a lawful basis to share the data in section 3 with Travel Code for the Integration Purposes, which for most employee data will be the performance of the employment contract or the Customer's legitimate interests (Article 6(1)(b) or (f) GDPR) and not employee consent; (b) it has given its employees, before the first run, the information required by Articles 13 and 14 GDPR

or equivalent law, naming Travel Code as recipient, the categories and purposes in section 3, the transfer described in section 5.3, and how to exercise their rights (Travel Code makes a template notice available in the Platform); (c) where local law requires it, it has consulted its works council or employee representatives before connecting the HR System; and (d) it is responsible for the accuracy of the data in its HR System.

4.3 Security. Travel Code protects data received through the integration under the Master Agreement and the DPA, including encryption in transit and at rest, encrypted credentials scoped to this integration, access to date of birth, sex and nationality restricted to the employee, travel bookers and authorised administrators, logging of administrative access, and the safeguards in section 1.3. Incidents are notified under the Master Agreement.

---

5. RETENTION, DELETION AND TRANSFERS

5.1 Copies kept for the integration. Travel Code keeps the latest copy of the data read from the HR System so that changes can be detected without reading everything again. This copy is deleted when the Customer disconnects the integration or withdraws the permission in section 6.

5.2 Employee accounts. Employee accounts created or updated by the integration are part of the Customer's Platform data and are kept and deleted under the Master Agreement, the DPA and the Data Retention Policy. Disconnecting the integration does not delete them. When an employee is archived, Travel Code deletes their date of birth, sex, nationality and personal contact data received through the integration 90 days after archiving, unless the Customer restores the employee or instructs otherwise. Booking, expense and invoice records are kept as the Data Retention Policy requires.

5.3 Transfers. The Platform is hosted in the United States. Personal data the integration receives from an HR System in the EEA, the UK or Switzerland is transferred under Travel Code's certification to the EU-U.S. Data Privacy Framework (and its UK and Swiss extensions) or, where that does not apply or the Customer requires it, under the Standard Contractual Clauses (Module 2) and UK Addendum incorporated in the DPA.

---

6. SEPARATE PERMISSION AND WITHDRAWAL

6.1 Separate permission. The integration runs only while the Customer's separate permission to receive employee data from its HR System is in force. That permission is asked for on its own screen and is not part of accepting this Schedule. It is the Customer's authorisation and instruction to Travel Code; it is not employee consent and does not replace the Customer's own lawful basis.

6.2 Record. The Platform keeps a record of who accepted this Schedule and who gave or withdrew the permission, and when, and shows it to the Customer's administrators.

6.3 Withdrawal. The Customer may withdraw that permission at any time in the Platform. Withdrawal stops the integration immediately, deletes the copies described in section 5.1 and ends this Schedule E. The rest of the Customer's agreement remains in force.

7. SUSPENSION AND TERMINATION

7.1 Travel Code may pause the integration if the HR System returns errors, if the credential stops working, or if continuing would risk the security or integrity of the Platform, and will tell the Customer in the Platform why.

7.2 Either party may end this Schedule E on notice in the Platform. Termination has the effects described in sections 5 and 6.3.

---

8. OPTIONAL: TRAVEL OFFERS FOR APPROVED LEAVE

8.1 Separate feature. This is an optional feature, not enabled by default. The Customer may switch it on through its own separate permission, which is not part of section 6 and may be withdrawn independently.

8.2 Employee opt-in. An employee receives offers only after opting in themselves in the Platform. The employee's opt-in is consent to Travel Code as controller under Article 6(1)(a) GDPR and applicable e-marketing law. It is not a condition of using the Platform and may be withdrawn at any time; every message carries a one-click unsubscribe.

8.3 Limits. For an opted-in employee Travel Code uses only the approved leave start and end dates, home location and work email, never the type of leave. Travel Code does not tell the Customer which employees opted in, received, opened or acted on an offer, or anything about any leisure booking.

8.4 Customer assessment. Before switching the feature on, the Customer confirms it has assessed the feature, including a legitimate-interest assessment for disclosing approved-leave dates to Travel Code, and updated its employee notice.