DATA PROCESSING ADDENDUM

This Data Processing Addendum (**DPA**) applies to Perk's Processing of Personal Data under the Agreement. The Key Terms (included at Section 3 of this DPA) illustrate the scope and details of the envisaged Processing.

This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

In the event of any conflict or inconsistency among the following documents forming part of our Agreement, the order of precedence will be: (1) the Order Form; (2) this DPA; (3) our Product Specific Terms and (4) our Service Terms.

To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA will be subject to our Service Terms, including, the exclusions and limitations, set forth in Clause 7 of our Service Terms.

This DPA was last updated on the 16 November 2026.

1 DEFINITIONS

"Anonymised Data" has the meaning given in Clause 4.2 of the Service Terms.

"**Audit**" and "**Audit Parameters**" are defined in Sections 10.3 and 10.4 below, respectively.

"**Audit Report**" is defined in Section 10.2 below.

"**Controller**" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

"**Customer Instructions**" is defined in Section 4.1 below.

"**Customer Personal Data**" means Personal Data in User data.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU)2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

"**Data Subject**" means an identified or identifiable natural person to whom Customer Personal Data relates.

"**EEA**" means European Economic Area.

"**Key Terms**" means the core details regarding the envisaged Processing of Customer Personal Data as specified by the Parties at Section 3 of this DPA.

"**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

"**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording,

organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

"Subprocessor" means a third party engaged by Perk to process Customer Personal Data under this DPA solely in connection with Perk's delivery of Services under the Agreement.

2 SCOPE AND DURATION

2.1. This DPA applies to Perk as a Processor of Customer Personal Data and to Customer as a Controller of Customer Personal Data.

2.2. This DPA commences on the Effective Date and terminates upon expiration or termination of the Agreement (or, if later, the date on which Perk has ceased all Processing of Customer Personal Data).

3 KEY TERMS

3.1. Categories of Data Subjects. Any User invited to the Platform and/or to receive the benefit of the Services by the Customer.

3.2. Categories of Customer Personal Data.

User Information (Platform level)	• Name, contact details (e.g., email address, phone number, business address), job and role information • Identification documents and verification data (e.g., passport, ID card, proof of residence, professional information) • Communications between Users and Perk customer support, including correspondence, feedback, and service requests
Travel & Events Module (only)	• Travel affiliation details (e.g., loyalty program numbers) • Travel history (e.g., hotel stays, flights, car rentals, trip itineraries) • Invoice-related content transferred by a Travel Supplier • Limited card details stored in connection with a User profile or cost centre they are assigned to (e.g., card type, last four digits, expiration date, bank account information)
Spend Module (only)	• Expense information (e.g., cost centre details, receipts, content uploaded by the Customer User which may include Personal Data) • Google location data for geocoding in trip creation (e.g. for calculating mileage allowance, no real-time tracking of Customer Users)
Perk Cards	• Cardholder data (e.g., name, address, phone number, business email address) for authentication or tokenisation • Card data (e.g., partial account number, expiration date, CVV, service code), account numbers, and related transaction data • Authentication data where required (e.g., 3DS information, card validation codes, PINs, sensitive authentication data processed by third parties) • Mobile payment data (e.g., Apple Pay or Google Pay device numbers and transaction codes)

3.3. Sensitive Categories of Data. Perk does not require Users to share special categories of Personal Data, and the Customer will inform its Users to do so only when necessary. Perk will delete such information, unless required to follow any reasonable User instructions (e.g., request for a special meal).

3.4. Nature and Purpose of the Processing. The provision of Services solely as contemplated in the Agreement, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.5. Duration of Processing. Perk will delete or anonymise Customer Personal Data within 30 days after termination, unless retention is required by Data Protection Laws, for dispute resolution, or to enforce Agreement. Certain records (including contracts, consent logs, invoices, and customer support interactions) may be retained for up to 6 years to meet legal obligations. Personal Data may be retained longer if legally required or necessary for litigation. Upon request, Perk will confirm deletion or anonymisation in writing. This DPA remains in effect until all such data has been deleted or anonymised.

4 PROCESSING OF PERSONAL DATA

4.1. Perk will Process Customer Personal Data as a Processor only:

a) in accordance with Customer Instructions; and

b) to comply with Perk's obligations under applicable Data Protection Laws.

"Customer Instructions" means: (i) Processing to provide the Services and perform Perk's obligations under the Agreement; and (ii) any reasonable instructions of Customer materially consistent with the terms of the Agreement.

4.2. Perk will notify Customer if it receives an instruction that Perk reasonably determines infringes Data Protection Laws (but Perk has no obligation to actively monitor Customer's compliance with Data Protection Laws).

4.3. Perk will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement. Perk will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

4.4. Perk and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data. Customer will comply with Data Protection Laws in its issuing of instructions to Perk. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Perk to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

4.5. The parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4.6. Nothing in this DPA restricts Perk's creation and use of Anonymised Data in accordance with Clause 4.2 of the Service Terms.

5 SUBPROCESSORS

5.1. Customer generally authorises Perk to engage Subprocessors to Process Customer Personal Data. Customer further agrees that Perk may engage its Affiliates as Subprocessors.

5.2. Perk will:

a) enter into a written agreement with each Subprocessor imposing data protection obligations substantially the same as those set out in this DPA; and

b) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Perk to breach any of its obligations under this DPA.

5.3. Perk will maintain an up-to-date list of its Subprocessors, as specified within its Trust Centre (the "**Subprocessor List**").

5.4. Perk may update the Subprocessor List from time to time. At least 30 days before any new Subprocessor Processes any Customer Personal Data, Perk will add such Subprocessor to the Subprocessor List and notify Customer through email or other means specified in the Order Form.

5.5. If, within 30 days after notice of a new Subprocessor, Customer notifies Perk in writing that Customer objects to Perk's appointment of such new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.

5.6. If the parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the affected Service for convenience and Perk will refund any prepaid, unused fees for the affected Service in respect of the terminated portion of the Term.

6 SECURITY

6.1. Perk will implement and maintain reasonable and appropriate technical and organisational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against security incidents, in accordance with the security measures set out in Perk's Trust Centre.

6.2. Perk will implement and follow procedures to detect and respond to security incidents. Perk will:

a) notify Customer without undue delay and, in any event, not later than forty-eight (48) hours after becoming aware of the incident affecting Customer; and
b) make reasonable efforts to identify the cause of the security incident, mitigate the effects and remediate the cause to the extent within Perk's reasonable control.

6.3. Upon Customer's request and taking into account the nature of the applicable Processing, Perk will assist Customer by providing, when available, information reasonably necessary for Customer to meet its security incident notification obligations under Data Protection Laws. Customer is solely responsible for complying with security incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any security incidents.

6.4. Customer acknowledges that Perk's notification of a security incident is not an acknowledgement by Perk of its fault or liability.

6.5. Security incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

6.6. Customer is responsible for reviewing the information made available by Perk relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

7 DATA PROTECTION IMPACT ASSESSMENT

7.1. Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Perk, Perk will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to

Customer's use of the Services, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

8 DATA SUBJECT REQUESTS

8.1. Upon Customer's request and considering the nature of the applicable Processing, Perk will assist Customer in complying with Customer's obligations under Data Protection Laws to respond to requests from Data Subjects to exercise their rights under Data Protection Laws, if Customer cannot reasonably fulfill such requests independently (including through use of the Services).

8.2. If Perk receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, Perk will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

9 DATA RETURN OR DELETION

9.1. During the Term, Customer may, through its administrative Users and the features of the Platform access, return to itself or delete Customer Personal Data.

9.2. Following termination or expiration of the Agreement, Perk will, in accordance with its obligations under the Agreement, return (at Customer's choice) or delete all Customer Personal Data from Perk's systems. Deletion will be in accordance with industry-standard secure deletion practices. Perk will issue a certificate of deletion upon Customer's request.

9.3. Notwithstanding the foregoing, Perk may retain Customer Personal Data:

a) as required by Data Protection Laws; or
b) in accordance with its standard backup or record retention policies,

provided that, in either case, Perk will (i) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data; and (ii) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

10 AUDITS

10.1. Perk will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Perk's obligations under this DPA and Data Protection Laws.

10.2. Perk will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (subject to confidentiality obligations). Customer may share a copy of Audit Reports with relevant government authorities as required upon their request. Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Sections 10.3 and 10.4 below.

10.3. Subject to the terms of this Section 10.3, Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Perk that is consistent with the Audit Parameters (an "**Audit**"). Customer may exercise its Audit right:

a) to the extent Perk's provision of an Audit Report does not provide sufficient information for Customer to verify Perk's compliance with this DPA or the parties' compliance with Data Protection Laws;
b) as necessary for Customer to respond to a government authority audit or a Data Subject exercising their rights; or
c) in connection with a security incident.

10.4. Each Audit must conform to the following parameters ("**Audit Parameters**"):

a) be conducted by an independent third party that will enter into a confidentiality agreement with Perk;
b) be limited in scope to matters reasonably required for Customer to assess Perk's compliance with this DPA and the parties' compliance with Data Protection Laws;
c) occur at a mutually agreed date and time and only during Perk's regular business hours;
d) occur no more than once annually (unless required under Data Protection Laws or in connection with a security incident);
e) cover only facilities controlled by Perk;
f) restrict findings to Customer Personal Data only; and
g) treat any results as confidential information to the fullest extent permitted by Data Protection Law.

11 CROSS-BORDER TRANSFERS

11.1. Perk processes Customer Personal Data:

a) in Ireland, Germany, Spain and Switzerland for Customers based in the EEA;
b) additionally in the United States for Customers based in the United States; and
c) additionally in the United Kingdom for Customers based in the United Kingdom.

11.2. Perk (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide its Services. If Perk engages in a Restricted Transfer, Perk shall implement appropriate safeguards, including:

a) ensuring that any recipient country has been deemed to provide an adequate level of protection by a competent authority; or
b) entering into Standard Contractual Clauses approved by the European Commission (or an equivalent instrument approved by a competent authority) and conducting a transfer impact assessment.

12 REGION SPECIFIC TERMS

12.1. To the extent that Perk Processes Customer Personal Data in California then for the purposes of understanding the CCPA, references made in this DPA to:

a) "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA;
b) the definition of "Data Subject" includes "consumer" as defined under the CCPA;
c) the definition of "Controller" includes "business" as defined under the CCPA; and
d) the definition of "Processor" includes "service provider" as defined under the CCPA.

12.2. Customer is providing the Customer Personal Data to Perk under the Agreement for the limited and specific business purposes of providing the Services as described in the Order Form and the Key Terms of this DPA and otherwise performing under the Agreement.

12.3. Perk will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.

12.4. Perk acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 10 (Audits) of this DPA to help to ensure that Perk's use of Customer Personal Data is consistent with Customer's obligations under the CCPA; (ii) receive from Perk notice and assistance under Section 8 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA; and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorised use of Customer Personal Data.

12.5. Perk will notify Customer promptly after it makes any determination that it can no longer meet its obligations under the CCPA.

12.6. Perk will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 12.2 above; or (ii) outside of the direct business relationship between Perk with Customer, except, in either case, where and to the extent permitted by the CCPA.

12.7. Perk will not sell or share Customer Personal Data received under the Agreement.

12.8. Perk will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.

13 ARTIFICIAL INTELLIGENCE

13.1. No training on Customer Personal Data. Perk shall not use, and shall ensure that its Subprocessors do not use, Customer Personal Data to train, fine-tune or otherwise improve any AI model, whether developed by Perk or a third party, without Customer's prior written consent.

13.2. Third-party AI providers. Where Perk engages a third-party AI provider to process Customer Personal Data to provide the Services, that provider shall be a Subprocessor under Section 5 (Subprocessors), and Perk shall ensure that its contract with that provider prohibits it from using Customer Personal Data to train or improve its models.

13.3. Customer-selected AI Clients. Where Customer or its Users connect an AI assistant, agent or other AI-powered application (an **"AI Client"**) to the Perk Platform through the Perk MCP server or the APIs, Section D of the Developer and Marketplace Terms applies, and the AI Client and its provider are not Subprocessors.