



PARTIES AND EXECUTION	
Entity details: <b>TRAVELPERK, S.L.U. (TravelPerk)</b> , a company incorporated in Spain with registered address in Carrer Almogàvers 154-164, 08018, Barcelona (Spain) and company ID B66484577.	
Signature:	Signature:
	
Name: Gabriel Silva	Name: Nellie Vail
Title: Legal Manager (Privacy)	Title: CFO
Date:	Date: 24-01-2024   07:14:33 PST

VARIABLES		
Parties' relationship	Controller to Processor	
Parties' roles	<b>TravelPerk</b> will act as the Controller (as defined in Section 1 of the Terms) <b>Supplier</b> will act as the Processor (as defined in Section 1 of the Terms)	
Contacts	Controller	Processor
	Data Protection Officer	Name: Jennifer Rosario
	Title: DPO	Title: CISO
	Email: dpo@travelperk.com	Email: security@spreedly.com
Main Agreement	Any agreements entered into by the parties from time to time for the provision of services by Supplier to TravelPerk.	
Term	This DPA will commence on the final date of signature and will continue for 30 days after the end of the Main Agreement.	
Breach Notification Period	Without undue delay after becoming aware of a personal data breach.	
Sub-processor Notification Period	30 days before the new sub-processor is granted access to Personal Data	
Liability Cap	the liability caps as per the Main Agreement.	
Governing Law and Jurisdiction	As per the Main Agreement.	
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data by the parties, including but not limited to those of: <ul style="list-style-type: none"><li>the European Economic Area (EEA)</li></ul>	

	<ul style="list-style-type: none"> <li>the United Kingdom (<b>UK</b>)</li> <li>the United States (<b>US</b>)</li> <li>Supplier's country of incorporation</li> </ul> <p>This includes, to the extent applicable, the European Union Regulation (EU) 2016/679, the Data Protection Act 2018, and the California Consumer Privacy Act of 2018 (<b>CCPA</b>)/California Privacy Rights Act of 2020 (<b>CPRA</b>), each as amended from time to time.</p>
<b>Services related to processing</b>	As described in the Main Agreement.
<b>Duration of processing</b>	<p>Supplier will retain Personal Data for the duration of the DPA, unless otherwise specified in writing by TravelPerk.</p> <p>Upon termination of the DPA, Supplier must, at the choice of TravelPerk, promptly delete or return all Personal Data to TravelPerk, unless retention of the Personal Data is required by applicable law.</p>
<b>Nature and purpose of processing</b>	Personal data processing activities include the storage and management of Personal Data in order for Supplier to provide its services as described in the Main Agreement.
<b>Personal Data</b>	The types of personal data processed are full name, email address, phone number and other personal data which may be provided by TravelPerk from time to time.
<b>Data subjects</b>	The individuals whose Personal Data will be processed by Supplier on behalf of TravelPerk.
<b>Special provisions</b>	<p>In this DPA, TravelPerk acts in his capacity as Controller. However, should TravelPerk be acting in his capacity as Processor on behalf of another Controller regarding any part of the Personal Data (e.g., personal data of TravelPerk users processed by TravelPerk on behalf of its customers): (i) the provisions of this DPA shall be entirely applicable (<i>mutatis mutandis</i>); (ii) Supplier shall be deemed a Sub-Processor; and (iii) to the extent a Transfer Mechanism is required, Module 3 [Processor-to-Processor] of the EU SCCs (as defined below), which is available at <a href="https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&amp;locale=en">https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&amp;locale=en</a> (as updated or replaced by the EU Commission from time to time) shall be deemed incorporated herein by reference and form an integral part of this DPA.</p>
<b>Transfer Mechanism</b>	<p>Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (as amended from time to time), for the transfer of personal data from the EEA or adequate country to a third country (the <b>EU SCCs</b> or the <b>Clauses</b>).</p> <p>International Data Transfer Addendum issued by the Information Commissioner's Office under Section 119A of the Data Protection Act 2018, effective from 21 March 2022 (<b>IDTA</b>), for the transfer of personal data from the UK to a third country (i.e., any non-EEA and non-adequate country).</p>

## ANNEX 1

	INFORMATION	SECURITY	GOVERNANCE
<b>Security measures.</b> Technical and organisational measures to ensure the security of Personal Data	A comprehensive information security program including a policy written in one or more readily accessible parts that: (1) contains technical, physical, administrative and procedural controls to provide for the security, confidentiality, integrity and availability of Personal Information		

and supplier systems; (2) protect against hazards or threats and unauthorized access or use of Personal Information; (3) controls identified risks; (4) addresses access, retention and transport of Personal Information, and (5) acceptable use. Designate an individual to manage and coordinate its written security policy and who is sufficiently trained, qualified and experienced to be able to fulfill those functions and any other functions that might reasonably be expected to be carried out by the individual as a security manager or officer.

**ASSET MANAGEMENT**  
Mechanisms exist to inventory system components that: (1) Accurately reflects the current system; (2) Is at the level of granularity deemed necessary for tracking and reporting; and (3) Includes organization-defined information deemed necessary to achieve effective property accountability.

All corporate laptops are full disk encrypted and wiped per industry standards when decommissioned.

All infrastructure equipment housing Customer Data resides within certified third-party data centers within AWS. AWS currently uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.

**BUSINESS CONTINUITY AND DISASTER RECOVERY**  
Plans and regular exercises to address business continuity of key people and processes along with disaster recovery plans for critical technology resiliency.

**CHANGE MANAGEMENT**  
Mechanisms exist to govern the technical configuration change control processes. Prior to implementing changes to the Platform Spreadly will assess the potential impact of such changes on Security and determine whether such changes are consistent with existing Security. No changes to the Platform or Security should be made which increase the risk of a Data Incidents or which would cause a breach of the Schedule.

**CLOUD SECURITY**  
Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.

**COMPLIANCE**  
Mechanisms exist to facilitate the identification and implementation of relevant legislative statutory, regulatory, and contractual controls.

**CONFIGURATION MANAGEMENT**  
Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.

**CONTINUOUS LOGGING AND MONITORING**  
Mechanisms exist to ensure that all systems used to store Customer Data are logged, monitored, and reviewed regularly.

**CRYPTOGRAPHIC PROTECTIONS**  
Spreadly will encrypt all sensitive cardholder data using appropriate encryption technology wherever it is stored or transmitted. Spreadly will use only strong, public encryption algorithms and reputable cryptographic implementations and will not employ any proprietary cryptography.

**DATA CLASSIFICATION AND HANDLING**  
Mechanisms exist to facilitate the implementation of data protection controls to ensure data and assets are categorized in accordance with applicable statutory, regulatory, and contractual requirements.

**ENDPOINT SECURITY**  
Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices including but not limited to (1) utilization of anti-malware technologies to detect and eradicate malicious code; (2) automatic updates of anti-malware technologies, including signature definitions; (3) ensuring that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged

users, unless specifically authorized by management on a case-by-case basis for a limited time period; and (4) utilization of host-based firewall software, or a similar technology, on all information systems, where technically feasible.

HR

SECURITY

As permitted by applicable Law, conduct reasonable background checks of any Spreadly personnel that will have access to Customer Data, including Criminal Record Bureau checks. Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.

IDENTIFICATION AND AUTHENTICATION

Mechanisms exist to (1) provide physical access controls, secure user authentication protocols, secure access control methods, and firewall protection; and (2) prevent terminated supplier personnel from accessing Personal Information and supplier systems by promptly terminating their physical and electronic access to such Personal Information. With respect to supplier systems and Personal Information: (1) maintain secure control over user IDs, passwords and other authentication identifiers; (2) maintain a secure method for selecting and assigning passwords and using authentication technologies such as token devices; (3) Restrict access to only active users/accounts; (4) block user access after multiple unsuccessful attempts to login or otherwise gain access; (5) assign unique user identifications plus passwords, which are not vendor supplied default passwords; and (6) require personnel to change passwords at regular intervals and whenever there is any indication of possible system or password compromise, and avoid re-using or cycling old passwords.

Duties and areas of responsibility of supplier personnel are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of supplier system or Personal Information.

INCIDENT

RESPONSE

Maintain policies and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and Data Incidents, and encouraging reporting actual or reasonably suspected Data Incidents, including: (1) training Supplier's personnel with access to Customer Data to recognize actual or potential Data Incidents and to escalate and notify the senior management of the foregoing; (2) mandatory post-incident review of events and actions taken concerning security of Customer Data.

MALICIOUS CODE MITIGATION SOFTWARE

Mechanisms exist to (1) implement and maintain software for Spreadly systems that detects, protects against, removes and remedies software or computer code designed to perform an unauthorized function on, or permit unauthorized access to, an information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs; (2) run mitigation software on at least a weekly basis; (3) update mitigation software automatically, including without limitation, obtaining and implementing the most currently available virus signatures.

NETWORK

SECURITY

Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network including but not limited to (1) up-to-date firewalls between supplier system, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks operated by Supplier that are not necessary for providing the Services to Customer, which are reasonably designed to maintain the security of Personal Information and supplier system; (2) implementation and management of a secure guest network.

PHYSICAL AND ENVIRONMENTAL SECURITY

Mechanisms exist to provide (1) reasonable restrictions on physical access to Customer Data and the Platform; and (2) physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and

	<p>applied.</p> <p>Policies concerning security for the storage, access, transportation and destruction of records and media containing Personal Information outside of business premises.</p> <p>PRIVACY</p> <p>Mechanisms exist to comply with applicable privacy laws, regulations, and notices.</p> <p>RISK MANAGEMENT</p> <p>Periodic and regular information security risk assessment and monitoring of Spreadly's information security program, Security and the Platform, at least annually, including: (1) identifying and assessing reasonably foreseeable internal and external threats and risks to the security, confidentiality, integrity and availability of Personal Information; (2) assessing the likelihood of, and potential damage that can be caused by, identified threats and risks; (3) regularly testing, monitoring and evaluating the sufficiency and effectiveness of Security and Data Incident response actions, and documenting same; (4) assessing adequacy of Spreadly personnel training concerning, and compliance with, Spreadly's information security program; (5) designing, implementing, adjusting and upgrading Security in order to limit identified threats and risks, and address material changes in technology, business and sensitivity of Customer Data; and (6) assessing whether such information security program is operating in a manner reasonably calculated to prevent unauthorized access or use of Customer Data; and (6) detecting, preventing and responding to attacks, intrusions and other system failures.</p> <p>SECURE ENGINEERING AND ARCHITECTURE</p> <p>Mechanisms exist to facilitate the implementation of industry-recognized security and privacy practices in the specification, design, development, implementation and modification of systems and services.</p> <p>SECURITY AWARENESS AND TRAINING</p> <p>Regular and periodic training of Spreadly personnel concerning: (1) Security; (2) implementing Spreadly 's information security program; and (3) the importance of personal information security.</p> <p>TECHNOLOGY DEVELOPMENT AND ACQUISITION</p> <p>Spreadly will adhere to industry best practices and standards for Secure Software Development Lifecycle (SSDLC), including all of, but not limited to, the following techniques: (1) Leveraging security guidelines from one or all the following industry best practices and standards – OWASP Top 10, SANS Top 25 and Cloud Security Alliance; (2) Consistently executed secure code reviews and testing either through manual peer review or via a code scanning solution; (3) Protection of test data and content and removal of test data and content before deployment to production; (4) System acceptance testing; and (5) System change control and approvals before deployment to production.</p> <p>THIRD PARTY MANAGEMENT</p> <p>Mechanisms exist to facilitate the implementation of third-party management controls including but not limited to: (1) reasonable steps and due diligence to select and retain third party suppliers that are capable of maintaining security consistent with the Schedule and complying with applicable legal requirements; (2) contractually requiring such suppliers to maintain such security; and (3) regularly assessing and monitoring third party suppliers to confirm their compliance with the applicable security required in the Schedule and by law.</p> <p>THREAT MANAGEMENT</p> <p>Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.</p> <p>VULNERABILITY AND PATCH MANAGEMENT</p>
--	---

	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information including but not limited to (1) software and firmware patching; (2) vulnerability scanning on a recurring basis; and (3) penetration testing conducted by an independent third party twice per year.
--	--

ANNEX 2	
<b>Sub-processors.</b> Current sub-processors	<a href="https://www.spreadly.com/gdpr-subprocessors">https://www.spreadly.com/gdpr-subprocessors</a>

## TERMS

### 1. What is this agreement about?

- 1.1 **Purpose.** The parties are entering into this Data Processing Agreement (**DPA**) for the purpose of processing Personal Data (as defined above).
- 1.2 **Definitions.** Under this DPA:
- (a) **adequate country** means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data,
  - (b) **Controller, data subject, personal data breach, process/processing, Processor and supervisory authority** have the same meanings as in the Data Protection Laws,
  - (c) **Business** and **Service Provider** have the same meanings as in the CCPA/CPRA, and
  - (d) **Sub-Processor** means another processor engaged by the Processor to carry out specific processing activities with Personal Data.

### 2. What are each party's obligations?

- 2.1 **Controller obligations.** Controller instructs Processor to process Personal Data in accordance with this DPA, and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow Processor to process Personal Data.
- 2.2 **Processor obligations.** Processor will:
- (a) only process Personal Data in accordance with this DPA and Controller's [and Processor's] instructions (unless legally required to do otherwise),
  - (b) not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA and the Main Agreement,
  - (c) inform Controller immediately if (in its opinion) any instructions infringe Data Protection Laws,
  - (d) use the technical and organisational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved,
  - (e) notify Controller of a personal data breach within the Breach Notification Period and provide assistance to Controller as required under Data Protection Laws in responding to it,
  - (f) ensure that anyone authorised to process Personal Data is committed to confidentiality obligations,
  - (g) without undue delay, provide Controller with reasonable assistance with:
    - (i) data protection impact assessments,
    - (ii) responses to data subjects' requests to exercise their rights under Data Protection Laws, and
    - (iii) engagement with supervisory authorities,
  - (h) if requested, provide Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA,
  - (i) allow for audits at Controller's reasonable request, provided that audits are limited to once a year and during business hours except in the event of a personal data breach, and
  - (j) return Personal Data upon Controller's written request or delete Personal Data by the end of the Term, unless retention is legally required.
- 2.3 **Warranties.** The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

### 3. Sub-processing

- 3.1 **Use of sub-processors.** Controller authorises Processor engage other processors (referred to in this section as **sub-processors**) when processing Personal Data. Processor's existing sub-processors are listed in Annex 2.
- 3.2 **Sub-processor requirements.** Processor will:
- (a) require its sub-processors to comply with equivalent terms as Processor's obligations in this DPA,
  - (b) ensure appropriate safeguards are in place before internationally transferring Personal Data to its sub-processor, and
  - (c) be liable for any acts, errors or omissions of its sub-processors as if they were a party to this DPA.
- 3.3 **Approvals.** Processor may appoint new sub-processors provided that they notify Controller in writing in accordance with the Sub-processor Notification Period.
- 3.4 **Objections.** Controller may reasonably object in writing to any future sub-processor. If the parties cannot agree on a solution within a reasonable time, either party may terminate this DPA.

### 4. International personal data transfers

- 4.1 **Instructions.** Processor will transfer Personal Data outside the UK, the EEA or an adequate country only on documented instructions from Controller, unless otherwise required by law.
- 4.2 **Transfer mechanism.** Where a party is located outside the UK, the EEA or an adequate country and receives Personal Data:
- (a) that party will act as the **data importer**,
  - (b) the other party is the **data exporter**, and
  - (c) the relevant Transfer Mechanism will apply.
- 4.3 **Additional measures.** If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.
- 4.4 **Disclosures.** Subject to terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):
- (a) challenge the request and promptly notify the data exporter about it, and
  - (b) only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

### 5. Other important information

- 5.1 **Survival.** Any provision of this DPA which is intended to survive the Term will remain in full force.
- 5.2 **Order of precedence.** In case of a conflict between this DPA and other relevant agreements, they will take priority in this order:
- (a) Transfer Mechanism,
  - (b) DPA,
  - (c) Main Agreement.
- 5.3 **Notices.** Formal notices under this DPA must be in writing and sent to the Contact on the DPA's front page as may be updated by a party to the other in writing.
- 5.4 **Third parties.** Except for affiliates, no one other than a party to this DPA has the right to enforce any of its terms.
- 5.5 **Entire agreement.** This DPA supersedes all prior discussions and agreements and constitutes the entire agreement between the parties with respect to its subject matter and neither party has relied on any statement or representation of any person in entering into this DPA.
- 5.6 **Amendments.** Any amendments to this DPA must be agreed in writing.
- 5.7 **Assignment.** Neither party can assign this DPA to anyone else without the other party's consent.
- 5.8 **Waiver.** If a party fails to enforce a right under this DPA, that is not a waiver of that right at any time.
- 5.9 **Governing law and jurisdiction.** The Governing Law applies to this DPA and all disputes will only be litigated in the courts of the Jurisdiction.

MODULE 2 SCHEDULE TO THE DATA PROCESSING AGREEMENT

PARTIES AND EXECUTION	
<b>Purpose.</b> This Schedule supplements the Data Processing Agreement entered into between the parties (the <b>DPA</b> ) to govern the international transfer of personal data. By signing below, the parties agree to the terms of this Schedule.	
<b>Data exporter</b>	<b>Data importer</b>
Entity details: TravelPerk, S.L.U., company incorporated in Spain with registered address in Carrer Almogàvers 154-164, 08018, Barcelona (Spain) and company ID B66484577.	Entity details: Spreadly, Inc.
Signature: 	Signature: 
Date:	Date: 24-01-2024   07:14:33 PST
Name: Gabriel Silva	Name: Nellie Vail
Title: Legal Manager (Privacy)	Title: CFO
Contact details: <a href="mailto:privacy@travelperk.com">privacy@travelperk.com</a>	Contact details: security@spreadly.com


VARIABLES	
<b>Docking</b>	Clause 7 of the Clauses does apply.
<b>Use of sub-processors</b>	Under clause 9 of the Clauses, the Parties select Option 2 (General written authorisation). The Sub-processor Notification Period shall apply.
<b>Redress</b>	Under clause 11 of the Clauses, the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall apply.
<b>Supervision</b>	No changes are made to clause 13(a) of the Clauses.
<b>Governing law</b>	Under clause 17 of the Clauses, the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of the country where the data exporter is based.



Jurisdiction	Under clause 18 of the Clauses (choice of forum and jurisdiction), the parties select the courts of the country where the data exporter is based.
--------------	---

APPENDIX TO THE CLAUSES

ANNEX I

A. LIST OF PARTIES	
Data exporter	
Name	As described in the Parties and Execution table at the beginning of this Schedule
Address	As described in the Parties and Execution table at the beginning of this Schedule
Contact person’s name, position and contact details	As described in the Parties and Execution table at the beginning of this Schedule
Activities relevant to the data transferred under these Clauses	As described in the Variables table at the beginning of the DPA
Signature and date	<i>Gabriel Silva</i>
Role	Controller
Data importer	
Name	As described in the Parties and Execution table at the beginning of this Schedule
Address	As described in the Parties and Execution table at the beginning of this Schedule
Contact person’s name, position and contact details	As described in the Parties and Execution table at the beginning of this Schedule
Activities relevant to the data transferred under these Clauses	As described in the Variables table at the beginning of the DPA
Signature and date	<div>DocuSigned by:  E7C3632005AC4CD... 24-01-2024   07:14:33 PST</div>
Role	Processor

B. DESCRIPTION OF TRANSFER	
<i>Term</i>	<i>Description</i>
<b>Data subjects.</b> Categories of data subjects whose personal data is transferred	As described in the Variables table in the DPA
<b>Personal data.</b> Categories of personal data transferred	As described in the Variables table in the DPA
<b>Sensitive data.</b> Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures	As described in the Variables table in the DPA
<b>Transfer frequency.</b> The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	As described in the Variables table in the DPA
<b>Nature of the processing</b>	As described in the Variables table in the DPA
<b>Purpose of the data transfer and further processing</b>	As described in the Variables table in the DPA
<b>Retention period.</b> The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Supplier will retain Personal Data for the duration of the DPA, unless otherwise specified in writing by TravelPerk.  Upon termination of the DPA, Supplier must, at the choice of TravelPerk, promptly delete or return all Personal Data to TravelPerk, unless retention of the Personal Data is required by applicable law.
<b>Sub-processor transfers.</b> For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As described in Annex 2 of the DPA

C. COMPETENT SUPERVISORY AUTHORITY	
<b>Supervisory authority.</b> Identify the competent supervisory authority/ies in accordance with Clause 13	The supervisory authority of the country where the data exporter is incorporated.

**ANNEX II**

TECHNICAL AND ORGANISATIONAL MEASURES	
<b>Measures.</b> Technical and organisational measures to ensure the security of the data	As described in Annex 1 of the DPA

**ANNEX III**

LIST OF SUB-PROCESSORS	
<b>Sub-processors.</b> The controller has authorised the use of sub-processors	As described in Annex 2 of the DPA

**ANNEX**

*to the*

**COMMISSION IMPLEMENTING DECISION**

**On standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

**STANDARD CONTRACTUAL CLAUSES**

**Controller to Processor**

**SECTION I**

*Clause 1*

***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*

***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clauses 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clauses 9(a), (c), (d) and (e);
  - (iv) Clauses 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clauses 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clauses 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### *Clause 4*

##### ***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### *Clause 5*

##### ***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### *Clause 6*

##### ***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### *Clause 7*

##### ***Docking clause***

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **SECTION II – OBLIGATIONS OF THE PARTIES**

#### *Clause 8*

##### ***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data

exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

#### *Clause 9*

##### ***Use of sub-processors***

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors within a reasonable timeframe in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### *Clause 10*

##### ***Data subject rights***

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.



*Clause 11*

**Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

**Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

**Supervision**

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### *Clause 14*

#### ***Local laws and practices affecting compliance with the Clauses***

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with

respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 15*

#### ***Obligations of the data importer in case of access by public authorities***

##### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

##### **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS**

*Clause 16****Non-compliance with the Clauses and termination***

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17****Governing law***

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Governing Law described in the Variables table of the DPA.

*Clause 18****Choice of forum and jurisdiction***

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (f) The Parties agree that those shall be the courts of the Jurisdiction described in the Variables table of the DPA.
- (g) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (h) The Parties agree to submit themselves to the jurisdiction of such courts.

INTERNATIONAL DATA TRANSFER ADDENDUM SCHEDULE

**Purpose.** This Schedule supplements the Data Processing Agreement entered into between the parties (the **DPA**) to govern the international transfer of personal data. By signing below, the parties agree to the terms of this Schedule.

PART 1: TABLES


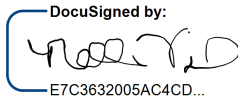
TABLE 1		
Start date	Date of the Parties' last signature to the DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Name: TRAVELPERK, S.L.U.  Address: Carrer Almogàvers 154-164, 08018, Barcelona (Spain).  Company number: B66484577	Name: Spreadly, Inc.  Address: 300 Morris St., Ste 400, Durham, NC 27701  Company number: 4387760
Key Contact	Name: DPO  Title: Data Protection Officer  Contact details: <a href="mailto:dpo@travelperk.com">dpo@travelperk.com</a>	Name: Jennifer Rosario  Title: CISO  Contact details: security@spreadly.com
Signatures	Signature:    Date:  Name: Gabriel Silva  Title: Legal Manager (Privacy)	Signature:    Date: 24-01-2024   07:14:33 PST  Name: nellie vail  Title: CFO

TABLE 2	
Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information

TABLE 3	
Appendix Information means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:	
Annex 1A	List of Parties: As described in the Module 2 Schedule to the DPA

<b>Annex 1B</b>	Description of Transfer: As described in the Module 2 Schedule to the DPA
<b>Annex II</b>	Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described in Annex II of the DPA
<b>Annex III</b>	List of Sub-processors: As described in Annex I of the DPA

**TABLE 4**

**Ending this Addendum when the Approved Addendum changes**

Which Parties may end this Addendum as set out in Section 19:  
 Exporter

## **PART 2: MANDATORY CLAUSES**

### **Mandatory Clauses**

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.