



ORDER FORM #Q-00267

**Spreedly, Inc.**  
300 Morris Street  
Suite 400  
Durham, NC 27701

**To:** Salvador Canelas  
**Customer Legal Name:** TravelPerk, S.L.U.  
**Tax ID:** B66484577  
**Billing Address:** Carrer Almogàvers 160, 08018,  
Barcelona, Spain  
**Sales Rep:** George Waugh

**Order Form Issued:** January 24, 2024  
**Offer Valid Until:** February 28, 2024

This Order Form is entered into between the entity identified above as “Customer” and Spreedly, Inc. (each a “Party” and collectively, the “Parties”) as of the last day it is signed (the “Order Form Effective Date”) and is subject to the Agreement (defined below) which is hereby incorporated by reference. For purposes of this Order Form, “Agreement” means the signed enterprise services agreement currently in force between the Parties, or, in the absence of an agreement, the Spreedly Terms of Service located at <https://www.spreedly.com/terms-of-service>.

In the event of any conflict between the terms of the Agreement and this Order Form, the Order Form will govern. Capitalized terms used but not defined in this Order Form have the meanings set forth in the Agreement or in the Documentation.

1. **Term.** The Initial Term of this Order Form is 12 months, after which this Order Form will automatically renew for successive 12-month periods (each, a “Renewal Term” and, together with the Initial Term, the “Term”) unless either party has provided written notice of its intent to not renew not less than 60 days prior to the expiration of the then-current Initial or Renewal Term. Each 12 months of service is a “Contract Year”. The services and Initial Term will begin February 28, 2024.

2. **Platform Fees.** For each Contract Year, Customer will pay Spreedly the “Annual Platform Fee” in Table 1 which entitles Customer to access and use the services of the Spreedly Platform as set out in the applicable Documentation, including:

- access to Level 1 PCI Compliant Card Storage and Tokenization;
- connections to any of Spreedly’s Supported Gateway integrations;
- use of existing 3DS2 services and gateway Supported Payment Methods; and
- all currently available Payment Method Distribution receiver endpoints.

Table 1	
Annual Platform Fee:	\$70,000.00
API Usage Fee:	\$19,000.00
Included API Calls – 1,000,000	
Cost per API Call – \$0.019	
Advanced Vault	\$10,000.00    See Table 2 for details
Professional Support	Included
<b>Committed Annual Fees</b>	<b>\$99,000.00</b>

3. **API Usage Fees.** . In addition to the Annual Platform Fee, Customer is pre-purchasing 1,000,000 API calls to the Spreedly Platform at a cost of \$0.019 per call (“API Usage Fee”) to be utilized during the Initial Term. Spreedly will invoice Customer monthly in arrears at the rate of \$0.019 for any additional API call more than the initial purchase volume of 1,000,000.



4. **Renewal Fees.** Except as otherwise agreed by the Parties in writing, this Order Form will automatically renew as described in Section 1 at the same committed API usage and the Annual Platform Fee and API Usage Fee will increase by 6% over the prior 12-months in each successive Renewal Term.

5. **Advanced Vault.** Spreedly's Advanced Vault service will be charged the greater of (i) the rate corresponding to the number of enrolled payment methods in each month of service as set out in Table 2 below or (ii) the minimum committed fee of \$833.34 per month. Costs are exclusive of fees imposed by the card associations and/or third-party service providers (e.g. card updates, tokenization, etc.) which will be passed through to Customer and are subject to change at any time. For the avoidance of doubt, Customer will still be charged the third party fee each time a payment card is updated. Spreedly will make reasonable efforts to notify Customers in advance of changes in third party fees.

Table 2			
Tier	# of Payment Methods	Monthly Fee Per Method	Minimum Monthly Fee
1	0 – 149,999	\$0.025	
2	150,000 – 1,499,99	\$0.0225	\$833.33
3	1,500,000 +	\$0.02	

By using Advanced Vault, Customer agrees that any updates to payment card information may be used by Spreedly to improve or provide payment services on its Platform. Customer authorizes Spreedly to act on Customer's behalf to (i) request and retain a Token Requestor ID from applicable card issuers, and (ii) use the Token Requestor ID to provision network tokens where available.

6. **Support Services.** Customer has selected Professional Support. Upon payment of the applicable fees, Spreedly will provide the technical Support Services in accordance with the Support Service Terms posted at <https://www.spreedly.com/support-services-terms> at the support level specified in this Order Form.

Spreedly will provide product and implementation support for Customer to integrate to the Spreedly Platform, including technical assistance with integration and data migration, and issue troubleshooting at no additional charge for up to three months following the Order Form Effective Date. Implementation support is available during Spreedly's normal business hours (9:00am-5:00pm EST) and workdays Monday through Friday excluding US holidays. Customer may request Spreedly perform integration work for an additional charge in a separate Statement of Work.

7. **Payments.** Customer will pay the Committed Annual Fees for the first Contract Year in full within 30 days of the Order Form Effective Date. Each subsequent annual payment of the Committed Annual Fees will be invoiced at least 30 days prior to the anniversary of the Order Form Effective Date ("Annual Renewal Date") and will be due and payable prior to the Annual Renewal Date. Customer will pay the applicable fees for Advanced Vaulting, and additional API Usages Fees (if any), will be invoiced monthly. All Fees are due and payable within 30 days of the invoice date are subject to the terms prescribed in the Agreement. All payments are subject to the terms prescribed in the Agreement.

Customer may elect to pay all amounts due under this Order Form either by:

(a) ACH payment or wire transfer to the following account:

Receiver: Webster Bank  
 ABA/Routing #: 211170101  
 SWIFT Code: WENAUS31  
 Beneficiary: 0024760830

Spreedly, Inc.  
 300 Morris Street, Suite 400  
 Durham, NC 27701  
 USA

or

(b) check delivered to the address specified in the relevant invoice.



CONFIDENTIAL

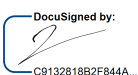
If Customer fails to make any payment when due then, in addition to all other remedies that may be available, Spreedly may charge interest on the past due amount at the rate of 1.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable law.



CONFIDENTIAL

The Parties have executed this Order Form by their duly authorized representatives in one or more counterparts, each of which will be deemed an original.

**Spreedly, Inc.**

By: 

Name: justin@spreedly.com

Title: CEO

Date: 2/28/2024

**TravelPerk, S.L.U.**

By: 

Name: Roy Hefer

Title: CFO

Date: 2/28/2024



## ENTERPRISE SERVICE AGREEMENT

This Enterprise Services Agreement ("Agreement") is entered by and between Spreedly, Inc., a Delaware corporation, ("Spreedly") and TravelPerk, S.L.U., a Spain Sociedad Limitada Unipersonal, ("Customer"). Spreedly and Customer are each a "Party" and collectively the "Parties". This Agreement is effective on the last date of signature by a Party in the signature block below ("Effective Date").

### Background

Spreedly develops, markets and provides to its customers a web-based payments orchestration and tokenization platform, which includes Spreedly's proprietary API integration (collectively, the "Platform"), which enables its customers to validate, tokenize and vault credit cards (and other payment types) and then transact with one or more of the payment gateways that are integrated to the Platform and/or third-party payment method receivers that Spreedly supports, and, where applicable, automatically update expired or lost credit cards (the "Permitted Use"). Customer desires to acquire a subscription to access and use the Platform for the Permitted Use, subject to the terms and conditions set forth herein.

### Agreement

The Parties agree for themselves, their successors and permitted assigns as follows:

1. Definitions. As used in this Agreement, the following terms will have the meanings set forth below:

1.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control of Customer, or any party with a direct or indirect shareholding or equity interest in Customer, as the case may be

1.2. "Agreement" means, collectively, this Enterprise Services Agreement, the Order Form(s), the Statements of Work, the Support Services Terms, and the Data Security Policy, in each case as amended from time-to-time.

1.3. "Card Associations" means MasterCard, VISA, American Express, Discover, JCB or any other credit card brand or payment card network for or through which Spreedly processes payment card transactions.

1.4. "Card Data" means any credit card data uploaded or otherwise received from Customer by or through the Platform for the purposes of being processed within the Platform.

1.5. "Claim" means any claim, suit, action, proceeding, or investigation by a governmental body.

1.6. "Customer Data" means Card Data and any other data or information that is uploaded or otherwise received from Customer by or through the Platform for the purposes of being processed within the Platform.



1.7. “Documentation” means the then-current online, electronic and written user documentation and guides, and instructional videos that Spreedly makes available to Customer at: <https://docs.spreedly.com/>, which describe the functionality, components, features or requirements of the Platform, as Spreedly may update from time-to-time in Spreedly’s discretion.

1.8. “Malicious Code” means any software, hardware or other technology, device or means, including any virus, worm, malware or other malicious computer code, the purpose or effect of which is to permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner any (a) computer, software, firmware, hardware, system or network or (b) any application or function of any of the foregoing or the security, integrity, confidentiality or use of any data processed thereby.

1.9. “Initial Order Form” means Order Form #1 executed by Customer and Spreedly concurrently with the execution and delivery of this Agreement.

1.10. “Intellectual Property Rights” means all patent rights, copyright rights, mask work rights, moral rights, rights of publicity, trademark, trade dress and service mark rights, goodwill, trade secret rights and other intellectual property rights as may now exist or hereafter come into existence, and all applications therefore and registrations, renewals and extensions thereof, under the Laws of any state, country, territory or other jurisdiction.

1.11. “Laws” means all laws, directives, rules and regulations.

1.12. “Losses” means any and all losses, damages, liabilities, deficiencies, judgments, settlements, costs and/or expenses (including reasonable attorneys’ fees).

1.13. “Order Form” means each ordering document which is substantially like the form in Schedule A that is executed by Customer and Spreedly that references this Enterprise Services Agreement. Each Order Form is hereby incorporated into this Agreement by reference, as amended from time-to-time by the Parties.

1.14. “PCI-DSS” means the Payment Card Industry Data Security Standard.

1.15. “Professional Services” means any consulting or professional services listed under a Statement of Work that are not included as part of the Support Services. Professional Services may include training, implementation, and configuration of the Platform.

1.16. “Statement of Work” means a statement of work executed by Customer and Spreedly that references this Enterprise Services Agreement, each of which is hereby incorporated into this Agreement by reference, as amended from time-to-time by the Parties.

## 2. Provision and Use of the Platform.

2.1. Authorization to Use the Platform. Subject to the terms of this Agreement, Spreedly authorizes Customer, during the Term and on a non-exclusive and non-transferable (except as permitted in Section 14.5) basis, to access and use the Platform solely for the Permitted Use. Customer acknowledges and agrees that Spreedly is not a payment gateway or merchant account provider and Spreedly does not assume any direct or indirect liability or responsibility for Customer’s agreements with payment gateways or merchant account providers supported on the Platform.

2.2. Lawful Use. Customer will access and use the Platform solely for lawful purposes and will not use it for any fraudulent, illegal or criminal purposes. Customer hereby grants Spreedly authorization to share information with law enforcement about Customer, Customer’s transactions and Customer’s Spreedly account, in each case if Spreedly reasonably suspects that Customer’s use of the Platform has been for an unauthorized, illegal, or criminal purpose. Further, Spreedly reserves the right to not store or submit any transaction Customer submits that Spreedly believes is in violation of this Agreement or applicable Law or otherwise exposes Spreedly or other Spreedly users to harm, including but not limited to, fraud, illegal, and other criminal acts.

2.3. Limitations and Restrictions. Customer will use commercially reasonable efforts to prevent unauthorized third-party access to or use of the Platform. Customer must not do any of the following:

- 2.3.1. modify, adapt, translate or create derivative works or improvements of the Platform or any portion thereof;
- 2.3.2. rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make available the Platform or any features or functionality of the Platform to any other person or entity for any reason, including as part of any time-sharing, service bureau or software as a service arrangement;



- 2.3.3. reverse engineer, disassemble, decompile, decode, adapt or otherwise attempt to derive, gain access to or discover the source code of the Platform or the underlying structure, ideas, know-how, algorithms or methodology relevant to the Platform;
- 2.3.4. input, upload, transmit or otherwise provide to or through the Platform any information or materials that are unlawful or injurious, or contain, transmit or activate any Malicious Code;
- 2.3.5. attempt to gain unauthorized access to, damage, destroy, disrupt, disable, impair, interfere with or otherwise impede or harm in any manner the Platform;
- 2.3.6. access or use the Platform in any way that infringes, misappropriates or otherwise violates any intellectual property right, privacy right or other right of any third party, or that violates any applicable Law; or
- 2.3.7. access or use the Platform for purposes of (A) benchmarking or competitive analysis, (B) developing, producing, marketing, distributing, licensing or selling any product or service that may compete with the Platform, or (C) disclosing to Spreedly's competitors, for any purpose, otherwise non-public information about the Platform.

2.4. Changes to the Platform. Spreedly may make any changes to the Platform (including, without limitation, the design, look and feel, functionality, content, material, information and/or services provided via the Platform) that Spreedly deems necessary or useful to improve the Platform or for any other reason, from time-to-time in Spreedly's sole discretion, and without notice to Customer; provided, however, that Spreedly will not make any such changes that will materially adversely affect its features or functionality available to Customer during the Term. Such changes may include upgrades, bug fixes, patches and other error corrections and/or new features (collectively, including related Documentation changes, "Updates"). All Updates will be deemed a part of the Platform governed by all the provisions of this Agreement pertaining thereto.

2.5. Subcontractors. Spreedly may, in Spreedly's discretion, engage subcontractors to aid Spreedly in providing the Platform and performing Spreedly's obligations under this Agreement, but Spreedly will remain fully liable to Customer for any act or omission by such subcontractors that would be a breach or violation of this Agreement. Spreedly may use Amazon Web Services, Microsoft Azure, Google Cloud Platform and/or such other reputable hosting provider that implements and maintains security programs, policies, procedures, controls and technologies in line with industry best practices (each a "Reputable Hosting Services Provider") for cloud-based infrastructure and hosting and storage services for the Platform, and such Reputable Hosting Services Provider will host and store certain portions of Customer Data that is processed through the Platform. Customer hereby specifically approves and consents to Spreedly's use of a Reputable Hosting Services Provider in the manner described and agrees that the Reputable Hosting Services Provider's security programs, policies, procedures, controls and technologies are consistent with industry best practices and comply with the requirements of the Data Security Policy. Spreedly represents and warrants that such delegation will not be to any providers on a government denied-party list in a U.S. embargoed country in violation of any applicable export law or regulation.

2.6. Beta Services. Spreedly may offer Customer access to beta services that are being provided prior to general release ("Beta Services"). Beta Services will be clearly designated as beta, pilot, limited release, developer preview, non-production, evaluation or by a similar description. Beta Services are for evaluation purposes and not for production use, are not considered "services" under this Agreement, are not supported, and may be subject to additional terms. Spreedly may discontinue Beta Services at any time in its sole discretion and may never make them generally available. ALL BETA SERVICES ARE PROVIDED "AS-IS" AND "AS AVAILABLE," WITHOUT WARRANTIES OF ANY KIND. Spreedly will have no liability for any harm or damage arising out of or in connection with the use of Beta Services. If Customer provides feedback ("Feedback") about the Beta Services, Spreedly will be free to use, disclose, reproduce, distribute, implement or otherwise commercialize all anonymised Feedback provided by Customer without obligation or restriction. For the Beta Services only, the terms of this Section 2.6 supersede any conflicting terms and conditions in the Agreement, but only to the extent necessary to resolve conflict.

2.7. Suspension of Services and Platform Access. Spreedly may suspend or deny Customer's access to or use of all or any part of the Platform and Support Services, without any liability to Customer or others, if (i) Spreedly is required to do so by Law or court order; or (ii) Customer has (A) failed to comply with Section 2.2 or 2.3, or (B) otherwise breached a material term of this Agreement and have failed to cure such breach within fifteen business (15) days after Spreedly provides written notice thereof to Customer. Spreedly's remedies in this Section are in addition to, and not in lieu of, Spreedly's termination rights in Section 10.

2.8. Customer Data Export; Customer Data Retention. Customer may elect at any time to perform an automatic export of any Card Data and/or other Customer Data to a third-party endpoint for which Spreedly supports third-party vaulting as set forth at Spreedly's website (currently: <https://docs.spreedly.com/guides/third-party-vaulting>). For any endpoint for which automatic export is not supported, Customer may request that Spreedly perform one (1) free-of-charge manual export during the Term, of any Card Data or other credit card or user information associated with Customer's account to a recipient designated by Customer, provided that the recipient has proven that it is





PCI-DSS compliant, and the transfer is not in violation of any applicable Laws. If Customer requires additional manual exports during the Term, each additional manual export will incur an export charge at Spreedly's then-current rates. Spreedly reserves the right to delete all of Customer's Card Data and any other Customer Data thirty (30) days after the effective date of termination of this Agreement (the "Data Transfer Window"). If Customer requires additional time to arrange the export of its Card Data to a PCI-DSS compliant third party, it may extend the Data Transfer Window for additional thirty (30) day periods by providing notice to Spreedly and continuing to pay a prorated portion of the applicable Fees set forth in the Order Forms.

### 3. Support Services and Availability.

3.1. Support Services. During the Term Spreedly will provide customer support services (the "Support Services") to Customer in accordance with Spreedly's Support Service Terms posted at Spreedly's website (currently: <https://www.spreedly.com/support-services-terms>) at the support level specified on the Order Form.

3.2. Availability. During the Term, Spreedly will make the Platform available for access and use by Customer in accordance with Spreedly's Availability Commitments posted at Spreedly's website (currently: <https://www.spreedly.com/support-services-terms>) corresponding to the support level specified on the Order Form. SPREEDLY'S SOLE OBLIGATION AND LIABILITY TO CUSTOMER FOR ANY FAILURE TO MEET THE AVAILABILITY COMMITMENTS ARE THE SERVICE CREDITS SPECIFIED IN THE SUPPORT SERVICE TERMS REFERENCED ABOVE.

4. Professional Services. If Customer and Spreedly execute a Statement of Work for Professional Services, the following additional terms will apply:

4.1. Scope of Services; Statements of Work. Subject to the terms of this Agreement, Spreedly will perform the training, consulting, advisory, implementation, configuration, customization and/or other professional services (the "Professional Services") that are mutually agreed upon and described in one or more Statements of Work.

4.2. Personnel. Spreedly reserves the right to determine which of Spreedly's personnel or subcontractors will be assigned to perform Professional Services, and to replace or reassign such personnel during the Term.

4.3. Customer Responsibilities. In connection with Spreedly's provision of the Professional Services, Customer will: (i) reasonably cooperate with Spreedly in all matters relating to the performance of the Professional Services; (ii) respond promptly to Spreedly's requests to provide direction, information, approvals, authorizations or decisions that are reasonably necessary for Spreedly to perform the Professional Services in accordance with the Statement of Work; (iii) provide the content, data and materials that Customer is required to provide as described in the Statement of Work; and (iv) perform those additional tasks and assume those additional responsibilities specified in the applicable Statement of Work ("Customer Responsibilities"). Customer understands and agrees that Spreedly's performance is dependent on Customer's timely and effective satisfaction of Customer Responsibilities.

4.4. Securing Rights. Customer will be solely responsible for securing all rights, consents, licenses or approvals to grant Spreedly access to or use of any third-party data, materials, software or technology necessary for Spreedly's performance of the Professional Services, other than with respect to any third-party materials included as part of the Platform or that Spreedly has otherwise agreed to provide as described in the Statement of Work. Spreedly will abide by the terms and conditions of such permissions, licenses or approvals, provided that Customer has provided to Spreedly written copies of such permissions, licenses or approvals prior to the commencement of the applicable Professional Services.

4.5. Ownership of Work Product. Unless Customer and Spreedly have otherwise expressly provided in a Statement of Work (including by making a specific reference to this Section 4.5), all Deliverables (as defined below) will be deemed to be a part of the Platform hereunder and therefore owned by Spreedly (pursuant to Section 8.1 below) and provided to Customer (pursuant to Section 2.1 above) under the terms of this Agreement. "Deliverables" means all results and proceeds of the Professional Services provided by Spreedly.

4.6. Acceptance of Deliverables. If Customer reasonably believes that any final Deliverable provided by Spreedly as part of Professional Services fails to conform in some material respect to the specifications set forth in the applicable Statement of Work, then Customer will provide Spreedly with a detailed written description of each alleged non-conformance within fifteen (15) business days after receipt of such Deliverable. In such an event, Spreedly will either confirm the non-conformance and commence work on making corrections to such Deliverable or inform Customer that Spreedly does not agree that a non-conformance exists and provide Customer with a written explanation for Spreedly's conclusion. If Spreedly does not agree that a non-conformance exists, Customer and Spreedly agree to work together in good faith to try to resolve the matter. If Spreedly does not receive a non-conformance notice from Customer within fifteen (15) business days after receipt of such Deliverable, such





Deliverable will be deemed to be accepted under this Agreement. Each Party will provide reasonable assistance and information to one another to assist in resolving any Deliverable non-conformance issues.

## 5. Confidentiality.

5.1. Confidential Information. In connection with this Agreement, each Party (as the "Disclosing Party") may disclose or make available its Confidential Information to the other Party (as the "Receiving Party"). "Confidential Information" means all proprietary, non-public information or materials of any character, whether written, electronic, verbal or otherwise furnished by the Disclosing Party or its directors, officers, employees, consultants, contractors, agents or advisors including those of its Affiliates that (i) is marked or otherwise identified as "Confidential" and/or "Proprietary" (or, if disclosed verbally, is reduced to writing and marked or identified as "Confidential" and/or "Proprietary" and forwarded to the other Party within thirty (30) days of oral disclosure) or (ii) should reasonably be understood from all the relevant circumstances to be of confidential or of a proprietary nature, including but not limited to, all (A) trade secrets, (B) financial information and pricing, (C) technical information, such as research, development procedures, algorithms, data, designs, and know-how, (D) individually identifiable personal information, (E) business and operational information, such as planning, marketing interests, pricing and products, and (F) customer lists and all related information. For avoidance of doubt, all non-public information related to the Platform (including without limitation, pricing information (e.g., price quotes) and the source code for the Platform and the methods, algorithms, structure and logic, technical infrastructure, techniques and processes used by Spreedly in developing, producing, marketing and/or providing the Platform) are Spreedly's Confidential Information, Customer Data is Customer's Confidential Information, and the terms of this Agreement and any Order Form or Statement of Work are the Confidential Information of both Parties.

5.2. Exclusions. Confidential Information of a Disclosing Party does not include information that the Receiving Party can demonstrate by written or other documentary records: (i) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information being disclosed or made available to the Receiving Party in connection with this Agreement; (ii) was or becomes generally known by the public other than by the Receiving Party's or any of its Representatives' (as defined in Section 5.3 below) noncompliance with this Agreement; (iii) was or is received by the Receiving Party on a non-confidential basis from a third party that was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; (iv) was or is independently developed by the Receiving Party without reliance upon any Confidential Information; or (v) to the extent it was or is independently developed by the Receiving Party with use of or reliance upon Residual Information (as defined below).

5.3. Protections. As a condition to being provided with any disclosure of or access to Confidential Information, the Receiving Party will: (i) not use the Disclosing Party's Confidential Information other than as necessary to exercise its rights or perform its obligations under and in accordance with this Agreement; (ii) except as may be permitted under the terms and conditions of Section 5.4 below, not disclose or permit access to such Confidential Information other than to its Affiliates and its Affiliates' respective officers, employees, directors, attorneys, accountants, professional advisors, contractors, subcontractors, agents and/or consultants (collectively, its "Representatives") who: (x) need to know such Confidential Information for purposes of the Receiving Party's exercise of its rights or performance of its obligations under and in accordance with this Agreement; and (y) have been informed of the confidential nature of the Confidential Information and the Receiving Party's obligations under this Agreement; (iii) safeguard the Confidential Information from unauthorized use, access or disclosure using at least the degree of care it uses to protect its own Confidential Information and in no event less than a reasonable degree of care; and (iv) promptly notify the Disclosing Party of any unauthorized use or disclosure of Confidential Information of which it becomes aware and take all reasonable steps to prevent further unauthorized use or disclosure. Each Party will be liable for any breach of this Agreement by its Representatives to whom it discloses Confidential Information.

5.4. Legally Required Disclosures. If a Receiving Party or one of its Representatives is required by any Law, rule or order of any governmental body or agency, or as otherwise necessary to maintain or comply with any regulatory certifications or requirements, to disclose any Confidential Information, such Receiving Party (i) will, to the extent legally permissible, give the Disclosing Party prompt notice of such request so that the Disclosing Party may (at its own expense) seek an appropriate protective remedy, and (ii) will, and will cause its Representatives to, cooperate with the Disclosing Party (at the Disclosing Party's expense) in the Disclosing Party's efforts to obtain any such protective remedy. In the event that the Disclosing Party is unable to obtain such a protective remedy, the Receiving Party or its Representatives, as applicable, will (A) furnish only that portion of the Confidential Information that the Receiving Party or its Representatives is required to disclose in the opinion of the Receiving Party's or its Representatives' outside counsel, (B) exercise reasonable efforts to assist the Disclosing Party (at the Disclosing Party's expense) in obtaining assurances that confidential treatment will be accorded the Confidential Information so required to be disclosed, and (C) give notice to the Disclosing Party of the information to be disclosed as far in advance of disclosure of the same as is reasonably possible and legally permissible.



5.5. **Ownership.** All Confidential Information will remain at all times the sole and exclusive property of the Disclosing Party and the Receiving Party will not acquire any rights in or to such Confidential Information by reason of its disclosure to the Receiving Party hereunder.

6. **Data Protection and Privacy.**

6.1. **Data Security.** During the Term, so long as Customer complies with this Agreement, Spreedly will implement safeguards to protect against anticipated threats or hazards to the security, confidentiality or integrity of Customer Data in accordance with Spreedly's Data Security Policy described in Schedule B, as amended from time-to-time (the "Data Security Policy").

6.2. **Data Privacy.** In the event that the Parties enter into an Order Form and/or SOW whereby Spreedly collects, accesses, processes, stores, transfers, transmits, uses, discloses or otherwise handles any Customer Data that includes "personal information," "personal data" or "personally identifiable information" as defined under applicable law (collectively "Personal Information"), Spreedly will store, use and otherwise process such Personal Information in all material respects in accordance with all applicable laws relating to the privacy and protection of the Personal Information involved ("Data Privacy Laws"), including but not limited to the California Consumer Privacy Act of 2018 and its implementing regulations (as amended, restated or supplemented from time to time, "CCPA") where applicable. Spreedly will not access, use, handle, maintain, process, dispose of, or disclose Personal Information other than as permitted or required under this Agreement or Data Privacy Laws. Spreedly will limit dissemination of Personal Information to its employees and subcontractors who (i) need to know the information to enable Spreedly to perform its obligations or exercise its rights under this Agreement, and (ii) are bound by confidentiality obligations substantially equivalent to those provided for in this Agreement. Upon Customer's written request Spreedly will cooperate with Customer as may be reasonably required to enable Customer to comply with Data Privacy Laws, including by reasonably assisting Customer in complying with individuals' rights in regards to their Personal Information under Data Privacy Laws. In furtherance of the foregoing, based on the Customer Data that Customer will process using the Platform or otherwise provide to Spreedly, if and to the extent Data Privacy Laws require additional clauses to be executed by Spreedly beyond those set forth in this Agreement, then Customer will notify Spreedly in writing of such requirement and Spreedly will in good faith review, negotiate and consider adding such clauses as an addendum to this Agreement. In the absence of such notice Customer represents and warrants that no additional clauses are required.

6.3. **CCPA Service Provider Compliance.** Spreedly and Customer both agree that Customer is a business and Spreedly is a service provider under CCPA. Spreedly will: (i) not retain, use or disclose personal information for any purpose (including any commercial purpose) other than for the specific purpose of providing the Platform and performing the Support Services and Professional Services contemplated by this Agreement; (ii) not retain, use or disclose personal information outside of the direct business relationship between Customer and Spreedly; and (iii) not sell the personal information to any third parties. Spreedly certifies that it understands and will comply with the restrictions, duties and obligations set forth in this Section 6.3. In the event that any consumer makes a request directly to Spreedly with respect to exercising its privacy rights under CCPA, Spreedly will promptly notify Customer and provide Customer with a copy of the consumer request, inform the consumer that the consumer's request cannot be acted upon because the request has been sent to a service provider, provide Customer with a copy of such response, and reasonably cooperate with Customer in its efforts to respond and act on the consumer's request in accordance with the requirements of CCPA, in each case unless legally prohibited from doing so. As permitted and provided by CCPA, nothing in this Section 6.3 will prohibit Spreedly from retaining, using or disclosing the personal information in connection with: (z) retaining or employing another service provider as a subcontractor, provided the subcontractor meets the requirements for a service provider under CCPA; (y) Spreedly's internal use to build or improve the quality of its Platform or services, provided that the use does not include building or modifying household or consumer profiles for use in providing services to another business, or correcting or augmenting data acquired from another source; (x) detecting data security incidents, or protecting against fraudulent or illegal activity; (w) complying with applicable laws; (v) complying with a civil, criminal or regulatory inquiry, investigation, subpoena, or summons by governmental authorities; (u) cooperating with law enforcement agencies concerning conduct or activity that Spreedly, Customer or a third party reasonably and in good faith believes may violate applicable law; or (t) exercising or defending legal claims. For purposes of this Section 6.3, the terms "business," "commercial purpose," "consumer," "personal information," "processing," "sell" and "service provider" will have the meanings given to such terms in CCPA.

7. **Fees and Payment.**

7.1. **Fees.** Customer will pay to Spreedly the fees and charges described in each Order Form and Statement of Work entered into by Customer and Spreedly (the "Fees") in accordance with such Order Form or Statement of Work



and this Section 7.

7.2. Taxes. If Spreedly is required by law to pay, withhold or deduct any taxes, levies, imports, duties, charges, fees or other amounts from Customer's payments, such amounts will be invoiced to and paid by Customer in addition to the Fees, unless Customer provides Spreedly with a valid exemption certificate from the corresponding authority. If Customer is required by law to withhold or deduct any portion of the Fees due to Spreedly (a "Customer Withholding"), Spreedly will be entitled to "gross-up" the applicable Fees in an amount equal to the Customer Withholding so that Spreedly receives the same Fees it would have received but for the withheld amounts required by law. Customer remains liable for the payment of all such Customer Withholdings, however designated, that are levied or based on Customer's use of the Platform.

7.3. Payment. Customer will make all payments in US dollars. Unless otherwise set forth in an applicable Order Form or Statement of Work, all invoiced amounts are due net thirty (30) days from the invoice date. Customer is responsible for providing complete and accurate billing and contact information and notifying Spreedly of any changes to that information.

7.4. Late Payment. If Customer fails to make any undisputed payment when due then, in addition to all other remedies that may be available to Spreedly (including Spreedly's rights under Section 2.7 and Section 9.3), Spreedly may charge interest on the past due amount at the rate of 1.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable law.

## 8. Ownership and Intellectual Property Rights.

8.1. Platform and Documentation. Customer acknowledges and agrees that Spreedly owns all right, title and interest in and to the Platform and the Documentation, including all Intellectual Property Rights therein and all derivative works thereof. Spreedly is not granting Customer any right, license or authorization with respect to the Platform or the Documentation, except as specifically provided in Section 2.1 above (and subject to the limitations and restrictions in Section 2.3 above). Spreedly reserves all rights not expressly granted to Customer in this Agreement.

8.2. Customer Data. As between Customer and Spreedly, Customer is and will remain the sole and exclusive owner of all right, title and interest in and to all Customer Data, including all Intellectual Property Rights therein, subject to the rights Customer grants to Spreedly in this Section 8. During the Term, Customer hereby grants to Spreedly and its subcontractors all such rights and permissions in or relating to Customer Data as are necessary to:

(i) provide the Platform to Customer; and (ii) enforce this Agreement and exercise Spreedly's rights and perform Spreedly's obligations under this Agreement.

8.3. Improvements. To the extent Spreedly makes any improvements to the Platform based upon Customer's use of the Platform, Customer agrees that Spreedly exclusively owns all right, title and interest in and to such improvements, including all related Intellectual Property Rights save for those incorporating the Customer's Intellectual Property.

8.4. Usage Data. Customer acknowledges and agrees that Spreedly may collect metadata and other statistical information regarding Customer's use of and the performance of the Platform ("Usage Data"). Usage Data does not contain and is not derived from Customer Data. Customer agrees that Spreedly may use Usage Data in connection with providing Support Services to Customer and for Spreedly's internal business purposes (such as monitoring, enhancing and improving the Platform), and that Spreedly may publish and share with third parties aggregated Usage Data that cannot, by itself or with other data, directly or indirectly, identify Customer, Customer's customers or clients or any other individual or entity.

Publicity Rights. During the Term, any use by either Party of the other's name, trademark and logo shall be subject to prior written approval (including by email).

## 9. Term and Termination.

9.1. Term. Unless otherwise terminated in accordance with this Agreement, the initial term of this Agreement will be for the duration specified in the Initial Order Form (the "Initial Term"). Thereafter, this Agreement will automatically renew for successive renewal terms (each, a "Renewal Term" and, together with the Initial Term, the "Term"), subject



to, and in accordance with, the terms of the Initial Order Form. Unless otherwise mutually agreed upon by the Parties, the term of each additional Order Form will be the same as the term set forth in the Initial Order Form.

9.2. Termination. In addition to any other termination rights described in this Agreement, this Agreement may be terminated at any time by either Party, effective when that Party provides written notice to the other Party: (i) at any time that there are no active and outstanding Order Forms and Statements of Work; or (ii) if the other Party materially breaches the terms of this Agreement (including, for avoidance of doubt, the terms of any Order Form or Statement of Work incorporated herein) and such breach remains uncured thirty (30) days after the non-breaching Party provides the breaching Party with written notice regarding such breach.

9.3. Effect of Termination. The exercise of any right of termination under this Agreement will not affect any rights of either Party (including rights to payment or reimbursement) that have accrued prior to the effective date of termination and will be without prejudice to any other legal or equitable remedies to which a Party may be entitled. If this Agreement is terminated or expires, then: (i) Spreedly will immediately discontinue Customer's access to the Platform; (ii) Customer will complete all pending transactions and stop accepting new transactions through the Platform; (iii) each Party will discontinue use of any trademarks and promptly remove any references and logos from the Other's website; and (iv) each Party will promptly return to the other or, if so directed by the other Party, destroy all originals and copies of any Confidential Information of the other Party (including all notes, records and materials developed therefrom).

9.4. Surviving Terms. Sections 1 (Definitions), 5 (Confidentiality), 7 (Fees and Payment), 8 (Ownership and Intellectual Property Rights), 9.3 (Effect of Termination), 10.c (Disclaimer of Warranties), 11 (Indemnification), 13 (Limitations of Liability), 14 (Miscellaneous) and this Section 9.4 will survive any expiration or termination of this Agreement along with any provision which by its nature or express terms should survive termination.

## 10. Representations and Warranties.

10.1. Mutual Representations. The Parties each represent and warrant as applicable that: (i) it is duly organized, validly existing and in good standing as a corporation or other entity under the laws of the jurisdiction of its incorporation or other organization; (ii) it has the full right, power and authority to enter into and perform its obligations under this Agreement; (iii) the execution of an Order Form by its representative has been duly authorized by all necessary corporate or organizational action of Customer; and (iv) when executed and delivered by both Parties, the Agreement will constitute the legal, valid and binding obligation of Customer, enforceable against Customer in accordance with its terms

10.2. Customer Representations. Customer represents and warrants that: (i) it will not knowingly use the Platform, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Platform; (ii) Customer's use of the Platform and its collection and use of all of Customer Data (including Customer's processing of Customer Data and/or any card authorization, credit, ticket only, capture or settlement request, decline transaction, or other related transaction, completed or submitted under Customer's account) will comply with (A) all applicable Laws, (B) the terms of service of the payment gateways, merchant service providers and/or API endpoints Customer connects with on the Platform; (C) the operating rules, bylaws, schedules, supplements and addenda, manuals, instructions, releases, specifications and other requirements, as may be amended from time-to-time, of any of the payment networks including Visa, MasterCard, American Express, Discover Financial Services, and any Affiliates thereof or any other payment network applicable to this Agreement; (D) PCI-DSS and PA-DSS, as applicable; and (E) any regulatory body or agency having jurisdiction over the subject matter thereof; (iii) Customer either owns, or has all rights, permissions and consents that are necessary to process, and to permit Spreedly, its subcontractors and the Platform to process as contemplated in this Agreement, all Customer Data and the credit card transaction related thereto; (iv) Spreedly's and its subcontractors' access to and use of Customer Data (including, for the avoidance of doubt, the Card Data and all personal data included with Customer Data) as contemplated by this Agreement does not and will not knowingly violate any applicable Law or infringe, misappropriate or otherwise violate any Intellectual Property Right, privacy right or other right of any third party.

10.3. Spreedly Representations. Spreedly represents and warrants that:

- 10.3.1. it will comply with all applicable rules and guidelines regarding service providers, third-party agents and processors as issued by the Card Associations (the "Card Rules"), as updated from time to time, and including Card Rules applicable to U.S. and international credit card transactions;
- 10.3.2. it will (A) be compliant with PCI-DSS and all other applicable standards and guidelines issued by the PCI Security Standards Council, LLC, (the "Council"); (B) validate its PCI-DSS compliance as required by the applicable Card Rules; (C) undergo annual PCI-DSS assessments by a Qualified Security Assessor; and (D) notify Customer if it becomes aware





that it is no longer in compliance with PCI-DSS. Spreedly will provide proof of its PCI-DSS compliance to Customer upon request and evidence of its successful completion of its annual assessments on its website (currently available at <https://www.spreedly.com/pci>);

- 10.3.3. the Platform will perform in accordance with the functional specifications set forth in the applicable Documentation. If Spreedly breaches this warranty, as Spreedly's sole obligation and liability to Customer and Customer's exclusive remedies, at its option shall be: (a) the correction of any portion of the Platform that fails to meet this warranty; (b) to obtain a reasonable procedure to circumvent the nonconformity; (c) a refund on a *pro rata* basis the share of any Fees prepaid by Customer for the portion of the applicable Term in which the Platform is non-conforming; or (d) where 10.3.3 (a) to (c) are not feasible, termination immediately of this Agreement immediately on notice
- 10.3.4. it will perform all Professional Services in a professional and workmanlike manner. If Spreedly breaches this warranty, Customer's remedies shall be either, the prompt re-performance of the non-conforming Services at no additional cost to Customer or termination of the Order Form in question or this Agreement as a whole.

10.4. Disclaimer of Warranties. EXCEPT FOR THE EXPRESS LIMITED WARRANTIES SET FORTH IN THIS AGREEMENT, THE PLATFORM AND ALL SERVICES PROVIDED BY SPREEDLY HEREUNDER ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS AND SPREEDLY HEREBY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHER, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING, NEITHER SPREEDLY NOR ANYONE ASSOCIATED WITH SPREEDLY, INC. REPRESENTS OR WARRANTS THAT THE PLATFORM WILL BE RELIABLE, ERROR-FREE OR UNINTERRUPTED, THAT DEFECTS WILL BE CORRECTED OR THAT THE PLATFORM WILL OTHERWISE MEET CUSTOMER'S NEEDS OR EXPECTATIONS.

## 11. Indemnification.

11.1. Spreedly Indemnification. Spreedly will defend Customer from and against any Claims brought by a third party, and will indemnify and hold Customer harmless from any Losses associated with such third party Claims arising from: (i) an allegation that the Platform (excluding Customer Data) infringes any U.S. patent, copyright or trademark of such third party, or misappropriate the trade secret of such third party (each, an "Infringement Claim"); (ii) a "Data Incident" that is caused by Spreedly's material breach of the Data Security Policy (as defined in Schedule B attached hereto); or (iii) Spreedly's failure to remain compliant with PCI-DSS.

11.2. Customer Indemnification. Customer will defend Spreedly and Spreedly's subcontractors and personnel from and against any Claims brought by a third party, and Customer will indemnify and hold Spreedly and Spreedly's subcontractors and personnel harmless from any Losses associated with such third party Claims, in each case to the extent the same are based on Customer's use of the Platform in violation of the terms of this Agreement and/or any applicable Law.

11.3. Indemnification Process. Each Party will promptly notify the other Party in writing of any Claim for which such Party believes it is entitled to be indemnified pursuant to Section 11.1 or 11.2. The Party seeking indemnification (the "Indemnitee") will cooperate with the other Party (the "Indemnitor") at the Indemnitor's sole cost and expense. The Indemnitor will promptly assume control of the defense and investigation of such Claim and will employ counsel of its choice to handle and defend the same, at the Indemnitor's sole cost and expense. The Indemnitee's failure to perform any obligations under this Section 11.3 will not relieve the Indemnitor of its obligations under this Section 11 except to the extent that the Indemnitor can demonstrate that it has been materially prejudiced as a result of such failure. The Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing. The Indemnitor will not enter into any settlement that imposes any liability or obligation on the Indemnitee without the Indemnitee's prior written consent.

### 11.4. Additional Terms for Infringement Claims.

- 11.4.1. Spreedly will have no liability or obligation with respect to any Infringement Claim to the extent based upon or arising out of: (A) access to or use of the Platform in combination with any hardware, system, software, network or other materials or service not provided or otherwise approved by Spreedly in the Platform Documentation; (B) use of the Service in the practice of a process or system other than that for which it was intended; or (C) any action taken by Customer relating to use of the Platform that is outside the scope of the rights and authorizations granted or otherwise in breach of this Agreement and/or any applicable Order Form.
- 11.4.2. If the Platform is, or in Spreedly's opinion is likely to be, the subject of an Infringement Claim, or if Customer's use of the Platform is enjoined or threatened to be enjoined, Spreedly may, at



Spreedly's option and Spreedly's sole cost and expense: (A) obtain the right for Customer to continue to use the allegedly infringing Platform as contemplated by this Agreement, (B) modify or replace the allegedly infringing Platform to make the Platform (as so modified or replaced) non-infringing, or (C) if Spreedly determine the remedies in clauses (A) and (B) are not commercially reasonable, then Spreedly may terminate the applicable Order Form upon written notice and without any liability to Customer and Spreedly will promptly refund to Customer on a *pro rata* basis the share of any Fees prepaid by Customer for the future portion of the applicable Term that would have remained but for such termination.

- 11.4.3. THIS SECTION 11 SETS FORTH CUSTOMER'S EXCLUSIVE REMEDIES, AND SPREEDLY'S SOLE OBLIGATION AND LIABILITY TO CUSTOMER OR ANY OTHER PERSON OR ENTITY, FOR ANY ACTUAL, THREATENED OR ALLEGED CLAIMS THAT THE PLATFORM (INCLUDING CUSTOMER'S USE THEREOF) INFRINGES, MISAPPROPRIATES OR OTHERWISE VIOLATES ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

12. Insurance. During the Term, Spreedly will maintain (i) commercial general liability insurance with at least \$1,000,000 per occurrence and (ii) "errors and omission" (tech and cyber coverage) insurance in an amount not less than \$5,000,000. Upon Customer's request, Spreedly will provide Customer with a certificate of insurance evidencing the same.

13. Limitation of Liability. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY LOST PROFITS, LOSS OF ANTICIPATED SAVINGS, WASTED EXPENDITURE, LOSS OF BUSINESS OPPORTUNITIES, REPUTATION OR GOODWILL, LOSS OR CORRUPTION OF DATA, OR ANY INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF BUSINESS PROFITS) ARISING OUT OF OR RELATING TO THIS AGREEMENT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THE TOTAL AND CUMULATIVE LIABILITY OF A PARTY ARISING UNDER OR IN CONNECTION WITH THIS AGREEMENT WILL NOT EXCEED THE AMOUNT OF FEES PAID TO SPREEDLY BY CUSTOMER DURING THE TWELVE-MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM, PROVIDED HOWEVER, THAT THIS LIMIT ON LIABILITY WILL NOT APPLY TO THE EXTENT THE LIABILITY IS A DIRECT RESULT OF THE FRAUDULENT, CRIMINAL OR GROSSLY NEGLIGENT OR MORE CULPABLE ACTS OR OMISSIONS OF THAT PARTY, FRAUDULENT REPRESENTATION, DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE OR ANY MATTER FOR WHICH IT WOULD BE UNLAWFUL FOR THE PARTIES TO EXCLUDE LIABILITY. THE LIMITATIONS IN THIS SECTION WILL APPLY EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

#### 14. Miscellaneous.

14.1. Entire Agreement. This Agreement and each Order Form and Statement of Work constitute the entire agreement, and supersede all prior negotiations, understandings or agreements (oral or written), between the Parties regarding the subject matter of this Agreement (and all past dealing or industry custom).

14.2. Amendment, Severability and Waiver. No change, consent or waiver under this Agreement will be effective unless in writing and signed by the Party against which enforcement is sought. Any delay or failure of either Party to enforce its rights, powers or privileges under this Agreement, at any time or for any period, will not be construed as a waiver of such rights, powers and privileges, and the exercise of one right or remedy will not be deemed a waiver of any other right or remedy. If any provision of this Agreement is determined to be illegal or unenforceable, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

14.3. Governing Law and Venue. This Agreement will be deemed to have been made in and will be governed by and construed in accordance with the laws of, the State of Delaware, without regard to its conflicts of law provisions. The sole jurisdiction and venue for actions related to this Agreement will be the state or federal courts located in the State of Delaware, and both Parties consent to the exclusive jurisdiction of such courts with respect to any such action.

14.4. Notices. All notices, instructions, requests, authorizations, consents, demands and other communications hereunder will be in writing and will be delivered by one of the following means, with notice deemed given as indicated in parentheses: (i) by personal delivery (when actually delivered); (ii) by overnight courier (upon written verification of receipt); (iii) by email (upon confirmation of receipt); or (iv) by certified or registered mail, return receipt requested (upon verification of receipt). In each case, such notices will be addressed to a Party at such Party's address set forth in the Initial Order Form (or such other address as updated by such Party from time-to-time by giving notice to the other Party in the manner set forth in this Section 14.4).

14.5. Assignment. Neither Party may assign, delegate or otherwise transfer its rights or obligations under this Agreement without the prior written consent of the other Party; provided that either Party may assign this Agreement



in its entirety without the other Party's consent to an entity that acquires all or substantially all of the business or assets of such Party to which this Agreement pertains, whether by merger, reorganization, acquisition, sale or otherwise. This Agreement will be binding upon, and inure to the benefit of, the successors and permitted assigns of the Parties.

14.6. No Third-Party Beneficiaries. This Agreement is for the sole benefit of the Parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Agreement.

14.7. Relationship of the Parties. The relationship between the Parties is that of independent contractors. Nothing contained in this Agreement will be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the Parties, and neither Party will have authority to contract for or bind the other Party in any manner whatsoever.

14.8. Force Majeure. Neither Party will be liable for any delays or non-performance of its obligations arising out of actions or decrees of governmental authorities, criminal acts of third parties, epidemics and/or pandemics as designated by governing authorities, earthquakes, flood, and other natural disasters, war, terrorism, acts of God, or fire, or other similar causes not within such Party's reasonable control (each, a "Force Majeure Event"). In the event of any failure or delay caused by a Force Majeure Event, the affected Party will give prompt written notice to the other Party stating the period of time the occurrence is expected to continue and use commercially reasonable efforts to end the failure or delay and minimize the effects of such Force Majeure Event. Either Party may terminate this Agreement if a Force Majeure Event affecting the other Party continues substantially uninterrupted for a period of thirty (30) days or more.

14.9. Equitable Remedies. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under Section 2.c (Limitations and Restrictions), Section 5 (Confidentiality) or Section 8 (Intellectual Property Rights) of this Agreement would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and that, in the event of such breach or threatened breach, the other Party will be entitled to equitable relief, including in a restraining order, an injunction, specific performance and any other relief that may be available from any court of competent jurisdiction, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity or otherwise.

14.10. Conflict in Terms. If there is a conflict between this Agreement and any Order Form or Statement of Work, the terms of such Order Form or Statement of Work will govern the provision of the Platform or the Professional Services involved; provided, however, that nothing in an Order Form or Statement of Work may modify or supersede anything in Sections 2.3 (Limitations and Restrictions), 4.5 (Ownership of Work Product), 8 (Ownership and Intellectual Property Rights), 10 (Representations and Warranties), 11 (Indemnification), 13 (Limitation of Liability), or 14 (Miscellaneous) of this Agreement unless an express cross-reference is made to the relevant provision of this Agreement in the applicable Order Form or Statement of Work and the Parties have expressly agreed in such Order Form or Statement of Work to modify or alter the relevant provision of this Agreement.

14.11. Counterparts. This Agreement may be executed in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. Counterparts may be delivered via facsimile, electronic mail (including pdf or any electronic signature complying with the U.S. federal ESIGN Act of 2000, e.g., [www.docusign.com](http://www.docusign.com)) or other transmission method and any counterpart so delivered will be deemed to have been duly and validly delivered and be valid and effective for all purposes.

[Signatures on Next Page]



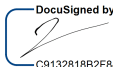


CONFIDENTIAL

The Parties have executed this Agreement by their duly authorized representatives in one or more counterparts, each of which will be deemed an original.

\_\_\_\_\_  
Spreedly, Inc.  
("Spreedly")

\_\_\_\_\_  
TravelPerk, S.L.U.  
("Customer")

DocuSigned by:  
  
C9132818B2F844A...


Authorized Signature  
justin@spreedly.com

Print Name  
CEO

Title

2/28/2024

Date

DocuSigned by:  
  
E55EA89905E640D...

Authorized Signature  
Roy Hefer

Print Name  
CFO

Title

2/28/2024

Date

**SCHEDULE A ORDER FORM**

[#]

**Spreedly, Inc.**  
300 Morris Street  
Suite 400  
Durham, NC 27701

**To:**  
**Customer Legal Name: Tax ID:**  
**Billing Address: Sales Rep:**

**Order Form****Issued:****Offer Valid****Until:**

This Order Form is entered into between the entity identified above as "Customer" and Spreedly, Inc. (each a "Party" and collectively, the "Parties") as of the last day it is signed (the "Order Form Effective Date") and is subject to the Agreement (defined below) which is hereby incorporated by reference. For purposes of this Order Form, "Agreement" means the enterprise services agreement (an "ESA") currently in force between the Parties.

In the event of any conflict between the terms of the Agreement and this Order Form, this Order Form will govern. Capitalized terms used but not defined in this Order Form have the meanings set forth in the Agreement or in the Documentation.

**1) Order Form Term****2) Platform Fees:****3) API Usage Fees:****4) Account Updater:****5) Payments:**

Customer may elect to pay all amounts due under this Agreement either by:

- (a) ACH payment or wire transfer to the following account:

Receiver: Webster Bank  
ABA/Routing #: 211170101  
SWIFT Code: WENAUS31  
Beneficiary: 0024760830  
Spreedly,  
Inc.  
300 Morris Street, Suite 400  
Durham, NC 27701  
USA

- (b) check delivered to the address specified in the relevant invoice.

**SAMPLE ONLY DO NOT SIGN**



## SCHEDULE B

### Data Security Policy

This Data Security Policy describes Spreedly's standard information security controls and is hereby incorporated into and made a part of the Enterprise Service Agreement between the Parties. Any capitalized terms used but not defined herein will have the meaning described in the Agreement. In the event of any conflict between the terms of the Agreement and this Data Security Policy, this Data Security Policy will govern with respect to the security measures in place for Customer Data.

#### A. Definitions.

A.1. "Data Incident" means a breach of Spreedly's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on the Platform. "Data Incidents" exclude unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

A.2. "Security" means Spreedly's technological, physical, administrative and procedural safeguards, including without limitation, policies, procedures, guidelines, practices standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is, in whole or part, to: (a) protect the confidentiality, integrity or availability of Customer Data and the Platform; (b) prevent the unauthorized use of or unauthorized access to the Platform; or (c) prevent a breach or malicious infection of Customer Data.

#### B. Data Security.

B.1. Security Controls. Spreedly uses industry-accepted technological, physical, administrative, procedural safeguards, methods and products, including without limitation, policies, procedures, guidelines, practices standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is to: (a) protect the confidentiality, integrity or availability of Customer Data and the Platform; and (b) prevent the unauthorized use of or unauthorized access to the Platform. Spreedly agrees that beginning on the Effective Date of the Agreement, Spreedly will employ and maintain, at a minimum, the reasonable and appropriate security controls listed in Attachment 1 attached hereto and incorporated by reference.

B.2. Data Ownership and Use Limitations. As between Spreedly and Customer, Customer is the owner of any and all Customer Data, including information provided by Customer's clients, customers or users, and Spreedly will have no ownership rights or interest in the Customer Data. Spreedly will use, process and handle Customer Data solely for the purpose of providing services under the Agreement and only per the instructions of Customer.

B.3. Data Deletion. Upon termination of the Agreement for which Spreedly is processing Customer Data, Spreedly will, upon Customer's request and subject to the limitations described in the Agreement, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement.

B.4. Data Tokenization. Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value called a token. Tokenization promotes security and efficiency between the Platform and connected payment gateways. When available, Spreedly may at its sole discretion tokenize applicable Customer Data for use within the Platform.

B.5. Third-Party Audit and Compliance. Spreedly undergoes annual PCI-DSS assessments by a Qualified Security Assessor and annual SOC 2 Type 2 audits performed by an external third-party. The copy of the most recent Attestation of Compliance with PCI-DSS is available at [www.spreedly.com/pci](http://www.spreedly.com/pci) and Spreedly will provide a copy of its most recent SOC 2 Type 2 upon Customer's request.

B.6. Use of Subcontractors. Prior to utilizing any subcontractor, vendor, or other third party, Spreedly will conduct a reasonable, documented investigation of such third party to ensure the third party can comply with the privacy, confidentiality and security requirements of Customer Data that are at least as protective of Customer Data as the requirements imposed on Spreedly under this Data Security Policy.

B.7. Additional Controls. Spreedly may update the security controls in Exhibit A from time to time upon notice to Customer and implement and maintain additional security controls in the event of any material changes to the Platform, available technology or systems, provided that such changes or additional controls will not materially reduce Spreedly's obligations under this Data Security Policy. In the event of any material change (including changes due to a change in applicable Law) which requires a change to all or a significant part of the security controls,



services or the Platform, the parties agree to make appropriate adjustments to the terms of the Agreement utilizing the amendment process.

C. Data Incident Response.

C.1. Response Actions. In the event of a Data Incident, Spreedly will:

- C.1.1. promptly conduct a reasonable investigation of the reasons for and circumstances of such Data Incident;
- C.1.2. take all reasonably necessary actions to prevent, contain, and mitigate the impact of, such Data Incident, and remediate such Data Incident;
- C.1.3. provide notice to Customer using the contact information identified in the most recent Order Form without undue delay and in any event within twenty-four (24) hours after the Spreedly confirms such Data Incident;
- C.1.4. promptly, and in no event more than two (2) Business Days after the Spreedly provides notice of a Data Incident provide a written report to Customer providing all relevant details concerning such Data Incident;
- C.1.5. collect and preserve all evidence concerning the discovery, cause, vulnerability, remedial actions and impact related to such Data Incident; and
- C.1.6. document the incident response and remedial actions taken in detail.

C.2. Data Incident Notice. Spreedly hereby authorizes Customer, in Customer's sole and absolute discretion, to provide notice of, and reasonably required information and documents concerning, any Data Incident, to third parties, including without limitations individuals or entities that may have been impacted by the breach.

C.3. Security Contacts. The following individuals will be the primary contacts for purposes of any coordination, communications or notices with respect to this Schedule, or any Data Incident:

<b>Customer Security Contact:</b>	<b>Spreedly Security Contact:</b>
Name: Bas Groeneweg	Name: Jennifer Rosario
Telephone: N/A	Telephone: 888-727-7750
Email: bas.groeneweg@travelperk.com	Email: security@spreedly.com

Each party will promptly notify the other if any of the foregoing contact information changes.

D. Monitoring and Reporting.

D.1. Records; Maintenance. Spreedly will, consistent with PCI-DSS and its security obligations in this Schedule and the Agreement, collect and record information, and maintain logs, planning documents, audit trails, records and reports, concerning its security, its compliance with this Schedule, Laws, Data Incidents, its storage, processing and transmission of Customer Data and the accessing and use of Customer Data on the Platform.

D.2. Customer Assessments. Upon reasonable notice to Spreedly, once per year during the Term, Customer (or any vendor selected by Customer subject to the conditions in this Schedule), may at Customer's sole cost, undertake an assessment and audit of security and Spreedly's compliance with this Schedule. The scope of such assessments and audits will be as mutually agreed between Spreedly and Customer but will not include penetration testing or any assessment that may adversely affect Spreedly's production environment.

D.3. Security Coordinator. Spreedly will assign a dedicated account manager that will act as the liaison between Customer and Spreedly to communicate compliance with this Schedule, coordinate Data Incident response and remedial action, and provide notice, reporting and other actions and duties as set forth in the Agreement. Spreedly will ensure that such individual is sufficiently trained, qualified and experienced to be able to fulfill these functions and any other related functions that might reasonably be expected to be carried out under this Schedule.

D.4. Information Requests.

- D.4.1. Spreedly will cooperate with Customer in responding to any party, non-party, or government or public authority request or demand made to Customer for information related to the services under the Agreement (including metadata). In the event that such



requests are served on Customer, Spreedly will provide Customer with access to such information in the format in which it is maintained in the ordinary course of business (or, on Customer's request, in any format necessary to satisfy such request).

- D.4.2. In the event a request or demand by any party, non-party, or government or public authority (in the form of a subpoena, court order or otherwise) is provided to or served on Spreedly for information related to the services under the Agreement (including Customer Data and metadata), Spreedly will, to the extent it may legally do so, promptly notify Customer's security contact (as specified in subsection 3.3) in writing by electronic mail.

E. Cooperation and Coordination. Spreedly agrees to reasonably cooperate and coordinate with Customer concerning: (a) Customer's investigation, enforcement, monitoring, document preparation, notification requirements and reporting concerning Data Incidents and Spreedly's and Customer's compliance with Privacy Laws; and (b) any other activities or duties set forth under this Schedule for which cooperation between Customer and Spreedly may be reasonably required.

F. Survival. Spreedly's obligations and Customer's rights in this Schedule will continue as long as Spreedly, or a third party for or on Spreedly's behalf, controls, possesses, stores, transmits or processes Customer Data, including after expiration or termination of the Agreement.

G. Data Processing Agreement. At the request of the Customer, Spreedly will enter into a data processing agreement that incorporates the European Commission Standard Contractual Clauses between Controllers and Processors, in accordance with the Agreement (or any similar agreement with respect to non-European Union countries) with Customer and its Affiliates in order to allow Customer to be transferred to Spreedly and any Spreedly Affiliate.



## Attachment 1: Specific Security Controls

Security Controls	
Information Security Governance	<p>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.</p> <p>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.</p>
Asset Management	<p>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.</p> <p>All corporate laptops are full disk encrypted and wiped per industry standards when decommissioned.</p> <p>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.</p>
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 Spreedly 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 Security Incident 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	Spreedly will encrypt all sensitive cardholder data using appropriate encryption technology wherever it is stored or transmitted. Spreedly 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 Spreedly 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	<p>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.</p> <p>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.</p> <p>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.</p>
Incident Response	Maintain policies and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and Security Incidents, and encouraging reporting actual or reasonably suspected Security Incidents, including: (1) training Supplier's personnel with access to Customer Data to recognize actual or potential Security 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 Spreedly 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	<p>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 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>





Privacy	Mechanisms exist to comply with applicable privacy laws, regulations, and notices.
Risk Management	Periodic and regular information security risk assessment and monitoring of Spreedly'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 Spreedly personnel training concerning, and compliance with, Spreedly'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.
Secure Engineering and Architecture	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.
Security Awareness and Training	Regular and periodic training of Spreedly personnel concerning: (1) Security; (2) implementing Spreedly 's information security program; and (3) the importance of personal information security.
Technology Development and Acquisition	Spreedly 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.
Third Party Management	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.
Threat Management	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.
Vulnerability and Patch Management	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.

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

	<p>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.</p> <p>HR SECURITY</p> <p>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.</p> <p>IDENTIFICATION AND AUTHENTICATION</p> <p>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.</p> <p>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.</p> <p>INCIDENT RESPONSE</p> <p>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.</p> <p>MALICIOUS CODE MITIGATION SOFTWARE</p> <p>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.</p> <p>NETWORK SECURITY</p> <p>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.</p> <p>PHYSICAL AND ENVIRONMENTAL SECURITY</p> <p>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>
--	--

	<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	<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>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


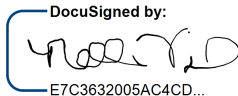
TABLE 1		
Start date	Date of the Parties' last signature to the DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Name: TRAVELPERK, S.L.U.  Address: Carrer Almogàvers 154-164, 08018, Barcelona (Spain).  Company number: B66484577	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.