DATA PROCESSING ADDENDUM

This DPA applies where, and to the extent that, Spreedly, Inc. ("Processor") processes personal data of data subjects on behalf of a customer (the "Controller") when providing access to its software platform, support services and/or professional services (collectively for the purposes of this DPA, the "Services") under one or more written agreements (collectively, the "Agreement"). This DPA may be supplemented with additional jurisdiction-specific clauses as described in Section 14(f) below.

In consideration of the mutual obligations set forth herein, the parties agree to the terms and conditions of this DPA, effective as of the earlier of the effective date of the Agreement or the processing of personal data.

1.   **Defined Terms**. For the purposes of this DPA only, the following terms have the meanings given to such terms below:

(a)   "Controller Personal Data" means any personal data processed by Processor on behalf of the Controller pursuant to the Agreement. For the avoidance of doubt, all Customer Data that constitutes personal data is Controller Personal Data.

(b)   "EEA" means the European Economic Area.

(c)   "Data Privacy Laws" means applicable laws relating to the privacy and protection of personal data, including without limitation (but only where applicable) GDPR.

(d)   "GDPR" means 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, including the recitals. Where personal data of data subjects in the United Kingdom is involved, "GDPR" more specifically means and refers to Regulation (EU) 2016/679, the General Data Protection Regulation together with and as implemented by the UK Data Protection Act of 2018 and the implementing rules or regulations that are issued by the UK Information Commissioner's Office ("ICO").

(e)   "personal data" means and includes "personal information" and "personal data" as defined under Data Privacy Laws.

(f)   "Restricted Transfer" means a transfer of Controller Personal Data from the Controller to Processor or any onward transfer of Controller Personal Data from Processor to a Subprocessor, in each case where such transfer would be prohibited by Data Privacy Laws in the absence of the parties' agreement to the Standard Contractual Clauses or another data transfer mechanism permitted by Data Privacy laws.

(g)   "Standard Contractual Clauses" means, collectively, (i) where personal data of data subjects in the EEA is involved, the standard contractual clauses set out in Commission Implementing Decision (EU)2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to GDPR (referred to herein more particularly as the "EU SCCs"), and (ii) where personal data of data subjects in the United Kingdom is involved, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018 (referred to herein more particularly as the "UK SCCs").

(h)   "Subprocessor" means any person or entity (excluding employees of Processor) appointed by or on behalf of Processor to Process Controller Personal Data on behalf of the Controller in connection with the Agreement.

(i)   Additionally, the terms "controller," "data subject," "personal data," "personal data breach," "process," "processor," and "supervisory authorities" (or their respective substantially corresponding equivalents under Data Privacy Laws) will have the meanings given to such terms under Data Privacy Laws.

2.   **Nature of Relationship**. The parties acknowledge and agree that the Controller is a controller and Processor is a processor under Data Privacy Laws.

3.   **Controller Representations and Warranties**. The Controller represents and warrants to Processor that, prior to transferring any Controller Personal Data to Processor for processing, asking Processor to collect Controller Personal Data on the Controller's behalf in connection with the Services, or otherwise providing or making available any personal data to Processor in connection with Processor's performance of the Services, the Controller has provided to the applicable data subjects every type of notice and obtained from the applicable data subjects every type of consent in each case as required by Data Privacy Laws pertaining to such disclosures of personal data to or collection of personal data on the Controller's behalf by Processor. The Controller will indemnify and hold harmless Processor from and against all claims, liabilities, fines, penalties, costs or other expenses, of any kind or nature whatsoever, arising out of the Controller's breach of this Section 3.

4.	**Description of Processing**.

(a)	Data Subjects: Personnel and customers of the Controller.

(b)	Categories of Data: With respect to personnel of the Controller, personal details, including information that identifies the data subject such as name, employer, address, e-mail, telephone number, location and other contact details. With respect to customers of the Controller, name, address, e-mail, telephone number, location, and billing and payment details such as bank account and credit or debit card numbers.

(c)	Special Categories of Data: None.

(d)	Nature and Purpose of Processing: All processing operations required to facilitate provision of Services to the Controller in accordance with the Agreement.

(e)	Frequency of Transfer (per Section 12 of this DPA): Continuously throughout the term of the Agreement.

(f)	Period of Retention of Personal Data: Except as otherwise provided in the Agreement or this DPA, in accordance with the retention policy of the Processor, provided that to the extent that any personal data is retained beyond the termination of the Agreement for back up or legal reasons, the Processor will continue to protect such personal data in accordance with the Agreement and this DPA.

(g)	For transfers to Subprocessors, the subject matter, nature and duration of the Processing: As described in Section 10 of this DPA.

5.	**Processing of Personal Data.** Processor will process Controller Personal Data only as needed to perform the Services and otherwise only on documented instructions from Controller (including, for the avoidance of doubt, as described in the Agreement), unless Processor is required to do so by applicable law to which Processor is subject, in which case Processor will inform the Controller of that legal requirement before processing (unless the applicable law prohibits providing such information to the Controller on important grounds of public interest). The Controller will ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Controller Personal Data, and that the processing of Controller Personal Data in accordance with the Controller's instructions will not cause Processor to be in breach of Data Privacy Laws or any other laws, rules or regulations applicable with respect to the Controller Personal Data. Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its processing of Controller Personal Data will meet the requirements of Data Privacy Laws and ensure the protection of the rights of the data subjects.

6.	**Confidentiality of Personal Data**. Processor will ensure that all persons (including Subprocessors) authorized to process Controller Personal Data have committed to keeping such Controller Personal Data confidential or are under an appropriate statutory obligation of confidentiality with respect to such Controller Personal Data. Processor will take steps to ensure that any natural person acting under the authority of the Processor who has access to Controller Personal Data does not process such Controller Personal Data except as needed to perform the Services or otherwise upon instructions from the Controller, unless the Processor is required to do so by applicable law to which Processor is subject.

7.	**Security of Personal Data**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, Processor will implement appropriate technical and organizational measures to ensure a level of security for Controller Personal Data appropriate to the risk, including in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Controller Personal Data transmitted, stored or otherwise processed. Such measures will include, *inter alia* as appropriate: (a) the pseudonymization or encryption of Controller Personal Data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services used to process Controller Personal Data, (c) the ability to restore the availability and access to Controller Personal Data in a timely manner in the event of a physical or technical incident, and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Additionally, such measures will include those set forth in the Processor's Data Security Policy attached as Schedule B to the Agreement.

8.	**Assistance and Cooperation**.

(a)	Processor will provide, at the Controller's cost, reasonable assistance to Controller in performing any data protection impact assessments and/or relevant consultations with supervisory authorities or other competent data privacy authorities, in each case to the extent required by Data Privacy Laws (such as, where applicable, GDPR Articles

35 or 36), and in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to, Processor and its Subprocessors.

(b)　　　Taking into account the nature of the Processing and the information available to Processor, Processor will, at the Controller's cost, assist Controller as Controller may reasonably require, including by appropriate technical and organizational measures, insofar as this is possible, in ensuring compliance with the Controller's obligations under Data Privacy Laws to appropriately secure and safeguard Controller Personal Data (such as, where applicable, pursuant to GDPR Article 32).

(c)　　　Taking into account the nature of the Processing, Processor will, at the Controller's cost, assist Controller as Controller may reasonably require, including by appropriate technical and organizational measures, insofar as this is possible, to enable the Controller to comply with requests by data subjects to exercise their rights under Data Privacy Laws. Processor will: (i) promptly notify the Controller if Processor receives a request from a data subject under Data Privacy Laws with respect to Controller Personal Data, and (ii) not respond to that request except on the written instructions of the Controller or as required by applicable law to which Processor is subject, in which case Processor will (to the extent permitted by applicable law) inform Controller of that legal requirement before Processor responds to the request.

9.　　　**Recordkeeping; Information and Audit Rights**. Processor will maintain all records pertinent to its processing of Controller Personal Data that are required by Data Privacy Laws, such as, where applicable, Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for the Controller) Processor will make such records available to the Controller upon the Controller's reasonable written request. Processor will make available to the Controller on the Controller's reasonable request all information necessary to demonstrate compliance with this DPA, and will, at the Controller's cost, allow for and cooperate with audits, including inspections, by the Controller or an auditor appointed by Controller in relation to the Processing of the Controller Personal Data by Processor, subject to the following:

(a)　　　Information disclosed to the Controller or its auditor or that is otherwise revealed in such records, inspections or audits will be the Confidential Information of Processor under the confidentiality provisions of the Agreement.

(b)　　　The Controller may request an audit by emailing success@spreedly.com.

(c)　　　Audits may not be conducted more than once per year or more frequently: (i) to the extent required by a supervisory authority, or (ii) in the event of and in connection with a particular personal data breach.

(d)　　　Audits will be conducted only during Processor's normal business hours and only with reasonable advance written notice of not less than 15 business days (except in the event of a personal data breach or if the Controller has a reasonable basis to believe (supported by substantial evidence) that Processor is in material non-compliance with this DPA, in which case advance notice will be not less than 72 hours).

(e)　　　Following the Processor's receipt of the Controller' written request to conduct an audit and/or inspection, the Processor and Controller will discuss and agree in advance on the reasonable scope, start date and duration of this audit, as well as any applicable security and confidentiality controls that may be required.

(f)　　　No such audit will include access to Processor's (or any Subprocessors') facilities or systems (e.g., computing infrastructure, servers, data storage mechanisms and infrastructure, audit logs, activity reports, system configuration, etc.) without Processor's prior written consent, except to the extent required by a supervisory authority.

(g)　　　The Processor may charge a fee (based on the Processor's reasonable costs) for any such audit. The Processor will provide the Controller with additional details of this fee including the basis of its calculation, in advance of the audit. Additionally, the Controller will be responsible for any fees charged by any third-party auditor appointed by the Controller for this audit.

In lieu of an audit, upon reasonable request by the Controller, but no more than once per year, Processor agrees to complete, within thirty (30) days of receipt, an audit questionnaire provided by the Controller regarding Processor's compliance with this DPA, of reasonable length and required detail (not to exceed a reasonably-estimated three person-hours to complete unless otherwise agreed to and subject to the payment of additional fees set forth in a separate written agreement by the parties), provided that any such questionnaire responses will be the Processor's Confidential Information under the confidentiality provisions of the Agreement.

10.　　　**Subprocessors**.

(a)　　　Processor will not engage any Subprocessor to process Controller Personal Data under the Agreement without written authorization from the Controller. Processor reserves the right to maintain its Subprocessor list through means such as publication of its Subprocessor list online, and the Controller hereby provides written

authorization for Processor to engage the Subprocessors listed online at https://www.spreedly.com/gdpr-subprocessors. Controller may receive notifications of new Subprocessors by emailing subprocessor@spreedly.com with the subject "Subscribe," and once subscribed in this manner Controller will receive notification of new Subprocessors before those Subprocessors are authorized to process Controller Personal Data on behalf of the Processor. Processor will send notice to Controller by email of any additional or replacement Subprocessors at least 10 days in advance of engaging any such additional or replacement Subprocessors to process Controller Personal Data under the Agreement. Controller may object to any such additional or replacement Subprocessor within 10 days of receiving such notice, provided that such objections are reasonable and on grounds relating to the protection or privacy of the Controller Personal Data involved in accordance with Data Privacy Laws or this DPA. Processor will use commercially reasonable efforts to resolve any such objection by the Controller, and the Controller will reasonably and in good faith cooperate with Processor in such efforts. If Processor cannot resolve the Controller's objection within a reasonable period of time following receipt of Controller's objection (such period of time not to exceed 60 days), and if Processor is unable to provide some or all of the Services without the use of the objected-to Subprocessor, then the Controller may terminate the applicable Services which cannot be provided by Processor without the use of the objected-to Subprocessor by providing written notice to Processor.

(b) Where Processor engages a Subprocessor for carrying out specific processing activities on behalf of the Controller with respect to Controller Personal Data, Processor will by contract impose on the Subprocessor substantially the same data protection obligations as set forth in this DPA. Where the Subprocessor fails to fulfil such data protection obligations, Processor will remain fully liable to the Controller for the performance of that Subprocessor's obligations.

(c) The Controller understands, acknowledges and agrees that the Processor is (and its Subprocessors may be) based in the United States and that the Processor provides (and the Subprocessors may provide) services under the Agreement from the United States, and the Controller hereby consents to the transfer of Controller Personal Data to the United States for Processing by the Processor and its Subprocessors in accordance with Section 12 below.

(d) Controller and Processor acknowledge that the Controller may engage a third-party payment gateway service provider and/or a third-party payment processing service provider to facilitate payment transactions in connection with the Agreement. Any such third parties engaged by the Controller will not be deemed a Subprocessor of the Processor for purposes of this DPA. Accordingly, nothing in this DPA obligates the Processor to enter into a data protection agreement with any such third party or to be responsible or liable for such third party's acts or omissions.

11. **Return or Deletion of Controller Personal Data**.

(a) Subject to Sections 11(b), 11(c) and 11(d) below, Processor will at Controller's request within thirty (30) days after the date of cessation of Services involving the Processing of Controller Personal Data, either; (i) return to the Controller the Controller Personal Data in a mutually-agreeable format; or (ii) delete and ensure the deletion of all copies of Controller Personal Data.

(b) Processor (and Processor's Subprocessors) may retain Controller Personal Data to the extent and for such period as is required by applicable law, rule or regulation, provided that Processor will ensure the continued confidentiality of all such Controller Personal Data, and will ensure that the Controller Personal Data are only accessed and used for the purpose(s) specified in the applicable law, rule or regulation requiring its retention. Additionally, solely to the extent not prohibited by Data Privacy Laws, Processor (and Processor's Subprocessors) may retain Controller Personal Data stored in electronic archived or backup systems until such copies are deleted in the ordinary course in accordance with Processor's data retention policies, provided that any such retained Controller Personal Data will remain protected to the standards of this DPA for so long as it is retained.

(c) Processor may retain and use for its business purposes any aggregated or de-identified data (i.e., data that is no longer personal data) created from or using Controller Personal Data, during and after termination of the Agreement.

(d) The Processor's obligations under this Section 11 will be subject to any agreed-upon post-termination data retrieval provisions in the Agreement.

12. **Restricted Transfers**. Subject to the remainder of this Section 12, the Controller (as "Data Exporter") and Processor (as "Data Importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from Controller to Processor. Processor will ensure that before it commences any Restricted Transfer to a Subprocessor, the Subprocessor will enter into the Standard Contractual Clauses (or variations of those Standard Contractual Clauses made under Section 14(e) or as otherwise proposed by the Subprocessor or Processor as long as such variations are compliant with Data Privacy Laws).

(a)   With respect to the EU SCCs, the same are incorporated by reference into this DPA on an unchanged basis save for the following:

(i)   Only "Module 2" of the EU SCCs applies;

(ii)   For the purposes of clause 9(a) of the EU SCCs, option 2 ("General Prior Authorisation") is selected and the specified time period is 10 days in advance;

(iii)   For the purposes of clause 11(a) of the E.U. Standard Contractual Clauses, the optional language is deleted;

(iv)   For the purposes of clause 13 of the EU SCCs: (i) if Controller is established in an EU Member State, the relevant supervisory authority acting as the competent supervisory authority is the supervisory authority of the EU Member State in which Controller is established, (ii) if Controller is not established in an EU Member State but has appointed a representative pursuant to GDPR Article 27(1), the relevant supervisory authority acting as the competent supervisory authority is the supervisory authority of the EU Member State in which Controller's representative is established, and (iii) if Controller is not established in an EU Member State and has not appointed a representative pursuant to GDPR Article 27(1), then the supervisory authority of one of the EU Member States in which the data subjects whose Controller Personal Data is transferred under the EU SCCs in relation to the offering of goods or services to them are located will act as competent supervisory authority. This paragraph will constitute "Annex I.C" for purposes of the EU SCCs;

(v)   For the purposes of clause 14(a) of the EU SCCs, the Assessment attached hereto as Appendix 1 is incorporated herein by reference.

(vi)   For the purposes of clause 17 of the EU SCCs, the governing law is Ireland;

(vii)   For purposes of clause 18(b) of the EU SCCs, the selection is Ireland; and

(viii)   The relevant party identification information from the Agreement and the description of processing in Section 4 of this DPA together will constitute "Annex 1" for the purposes of the EU SCCs. Sections 6 and 7 of this DPA will constitute "Annex 2" for the purposes of the EU SCCs.

(b)   With respect to the UK SCCs, the same are incorporated by reference into this DPA on an unchanged basis save for the following:

(i)   In Table 2, the selections made are those that match the EU SCCs as described and detailed in clause (a) of this Section 12;

(ii)   In Table 4, both "importer" and "exporter" are selected; and

(iii)   The relevant party identification information from the Agreement, the description of processing in Section 4 of this DPA, and Sections 6 and 7 of this DPA will be incorporated into (and will constitute) Tables 1 and 3 of the UK SCCs, as applicable.

13.   **Personal Data Breach**. Taking into account the nature of processing and the information available to the Processor, Processor will reasonably assist the Controller in the Controller's efforts to comply with its obligations regarding personal data breaches as set forth in Data Privacy Laws, such as, where applicable, GDPR Articles 33 and 34. If any Controller Personal Data is subject to any personal data breach Processor will, upon becoming aware of the personal data breach, without undue delay notify the Controller, take reasonable steps to contain and counteract the personal data breach and minimize any damage resulting from the personal data breach, and provide Controller with sufficient information to allow the Controller to meet any obligations to report to supervising authorities or inform the applicable data subjects of the personal data breach to the extent required under Data Privacy Laws. Processor will cooperate, at the Controller's cost, to assist Controller in the investigation, mitigation and remediation of each such personal data breach.

14.   **Miscellaneous**.

(a)   Subject to the following sentence of this Section 14(a), in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA will prevail. In any event, Processor's liability under this DPA, including for breach or other failure under this DPA by Processor or its Subprocessors, will be (to the maximum extent permitted under Data Privacy Laws, the Standard Contractual Clauses and other applicable law) subject to the exclusions and limitations of liability provided for in the Agreement as if this DPA were a part of the Agreement, *ab initio*.

(b)   To the extent this DPA is not governed exclusively by Data Privacy Laws, it will be governed by and construed in accordance with the laws selected pursuant to the governing law provision set forth in the Agreement.

(c)   This DPA constitutes the entire understanding of the parties with respect to the subject matter hereof and supersedes all prior agreements, oral or written.

(d)   Except as expressly stated in Data Privacy Laws or the Standard Contractual Clauses attached hereto, the parties to this DPA do not intend to create any rights in any third parties.

(e)   The parties agree that, to the extent required under Data Privacy Laws, such as due to legislative changes, court decisions, and/or to reflect measures or guidance from supervisory authorities, including, without limitation and only where applicable, the adoption of standards for contracts with processors according to GDPR Article 28(7) or (8) or the invalidation, amendment, replacement or repeal of a decision adopted by the EU Commission or ICO in relation to international data transfers on the basis of GDPR Article 45(3) or Article 46(2) GDPR or on the basis of Article 25(6) or 26(4) of EU Directive 95/46/EC, such as, in particular, with respect to the Standard Contractual Clauses or similar transfer mechanisms, the Controller may request reasonable changes or additions to this DPA to reflect applicable requirements. If the Controller makes a request to change or supplement this DPA pursuant to this Section 14(e), the Controller and Processor will in good faith negotiate such changes and additions (including, where applicable, providing for Controller's reimbursement of Processor's costs and expenses for undertaking additional obligations) and the Processor will not unreasonably withhold or delay agreement to any variations to this DPA.

(f)   Controller and Processor hereby accept and agree to, and where and as applicable will adhere to, the clauses that appear in the following attachments:

- Attachment 1 – Compliance with the Federal Act on Data Protection of the Swiss Confederation (FADP)
- Attachment 2 – Compliance with U.S. State Consumer Privacy Laws
- Attachment 3 – Compliance with the Brazilian Data Protection Law (LGPD)
- Attachment 4 – Compliance with Argentina's Pending Data Protection Law

(g)   Based on the Customer Data that Controller will process using the Platform or otherwise provide to Processor, if and to the extent Data Privacy Laws require additional clauses to be executed by Processor beyond those set forth in this DPA, then Controller will notify Processor in writing of such requirement and Processor will in good faith review, negotiate and consider adding such clauses as an additional addendum to the Agreement. In the absence of such notice Controller represents and warrants that no additional clauses are required.

Attachment 1

**Compliance with the Federal Act on Data Protection of the Swiss Confederation
as Revised Effective September 1, 2023 ("FADP")**

---

1. This Attachment 1 applies only to any processing of personal data that has actual or potential effects in the Swiss Confederation.

2. All provisions of the above DPA are incorporated and restated in this Attachment 1 in their entirety, except as specifically amended or modified below.

3. References to Data Privacy Laws in the DPA will mean and include (but only where applicable) FADP.

4. Section 12(a) of the DPA is supplemented and amended as follows, as and to the extent required by the FADP:

    (a) All references to the GDPR in Section 12(a) and in the EU SCCs are to be understood as references to the FADP, which governs all data transfers from the Swiss Confederation, and which permits the use of the EU SCCs. This provision will constitute the Annex required by the Federal Data Protection and Information Commissioner ("FDPIC") in its guidance issued August 27, 2021.

    (b) The term "Member State" must not be interpreted in such a way as to exclude data subjects in the Swiss Confederation from the possibility of suing for their rights in their place of habitual residence, in accordance with Clause 18(c) of the EU SCCs. This provision will constitute the Annex required by the FDPIC in its guidance issued August 27, 2021.

    (c) Section 12(a)(iv) is amended to state: "For the purposes of clause 13 of the EU SCCs, the FDPIC of the Swiss Confederation is the competent supervisory authority. This paragraph will constitute 'Annex I.C' for purposes of the EU SCCs."

    (d) In Sections 12(a)(vi) and 12(a)(vii), "Ireland" is replaced by "Swiss Confederation."

5. Section 12(b) of the DPA is deleted.

Compliance with U.S. State Consumer Privacy Law

This Attachment 2 applies where, and to the extent that, Processor processes personal information of consumers within one or more U.S. States that have enacted consumer privacy laws applicable to the Services.

Notwithstanding anything to the contrary elsewhere in the DPA, where the California Consumer Privacy Act of 2018 and its implementing regulations, as amended effective January 1, 2023 by the California Privacy Rights Act and its implementing regulations (the two laws collectively, as amended, restated or supplemented from time-to-time, the "CCPA/CPRA") applies, the terms "business," "combine," "commercial purpose," "consumer," "contractor," "personal information," "processing," "sell," "share," and "service provider" will have the meanings given to such terms in CCPA/CPRA; and where any of the state privacy laws listed below and their respective implementing regulations (each, an "Other State Law," and, collectively, the "Other State Laws") apply, the terms "consumer," "controller," "processing," "processor," "sell" (and its corresponding "sale") and "targeted advertising" will have the meanings given to such terms in the applicable Other State Law, and the term "personal information" will have the same meaning as the term "personal data" as such term is defined in the applicable Other State Law. The Other State Laws are:

- The Virginia Consumer Data Protection Act, effective January 1, 2023 (as amended, restated or supplemented from time-to-time, the "VCDPA");
- The Colorado Privacy Act, effective July 1, 2023 (as amended, restated or supplemented from time-to-time, the "CPA");
- The Connecticut Personal Data Privacy and Online Monitoring Act, effective July 1, 2023 (as amended, restated or supplemented from time-to-time, the "CPDPOMA"); and
- The Utah Consumer Privacy Act, effective December 31, 2023 (as amended, restated or supplemented from time-to-time, the "UCPA").

In consideration of the mutual obligations set forth herein, the parties agree to the terms and conditions of this Addendum.

1.   The parties acknowledge and agree that the Controller is a business and Processor is a service provider or contractor to the Controller under the CCPA/CPRA, and Controller is a controller and Processor is a processor under the Other State Laws. Controller represents, warrants and covenants that it has complied and it will comply with the CCPA with respect to all personal information of consumers that Controller has transferred or made available to Processor and its Subprocessors, or that Controller has asked Processor or its Subprocessors to collect on Controller's behalf for processing in connection with the Services. The Controller will indemnify and hold harmless Processor from and against all claims, liabilities, fines, penalties, costs or other expenses, of any kind or nature whatsoever, arising out of the Controller's breach of this Section 1.

2.   In its processing of personal information of consumers that the Controller has transferred to Processor for processing, that Processor may have access to, or that Processor has collected on the Controller's behalf, in each case in connection with the Services, Processor will comply with all requirements of the CCPA/CPRA that are applicable to service providers and contractors and all requirements of the applicable Other State Laws that are applicable to processors. Without limiting the foregoing, during the term of the Agreement and thereafter, Processor will: (i) not retain, use or disclose the personal information for any purpose (including any commercial purpose) other than for the specific purpose of performing the Services contemplated by the Agreement; (ii) not retain, use or disclose the personal information outside of the direct business relationship between Processor and the Controller; (iii) not sell or (where CCPA/CPRA applies) share the personal information to any third parties; and (iv) not combine the personal information that Processor receives from, or on behalf of, Controller with personal information that Processor receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Processor may combine such personal information (1) for the specific purpose of providing the Services contemplated by the Agreement or (2) to perform any other permitted business purpose under CCPA/CPRA and/or the Other State Laws, as applicable. Processor certifies that it understands and will comply with the restrictions, duties and obligations set forth in this Section 2.

3.   Where not prohibited by applicable law, nothing in this Addendum will prohibit Processor from retaining, using or disclosing the personal information in connection with: (i) retaining or employing another service provider, contractor or subcontractor (as applicable), provided the service provider, contractor or subcontractor meets the requirements for a service provider, contractor or subcontractor under the CCPA/CPRA or Other State Law, as applicable; (ii) internal use by Processor to build or improve the quality of its 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; (iii) detecting data security incidents, or protecting against fraudulent or illegal

activity; (iv) complying with federal, state or local laws; (v) complying with a civil, criminal or regulatory inquiry, investigation, subpoena, or summons by federal, state or local authorities; (vi) cooperating with law enforcement agencies concerning conduct or activity that the Controller, Processor or a third party reasonably and in good faith believes may violate federal, state or local law; or (vii) exercising or defending legal claims.

4.   If Processor authorizes any Subprocessor to process, retain or use any personal information received from the Controller, accessed in connection with the Services or collected on the Controller's behalf in connection with the Services, then prior to any disclosure of such personal information to such Subprocessor, Processor will enter into a written agreement with such Subprocessor that includes all required or necessary terms to ensure that such Subprocessor is deemed a service provider or contractor within the meaning of the CCPA/CPRA or a subcontractor within the meaning of any applicable State Law.

5.   To the extent this Addendum is not governed exclusively by CCPA/CPRA or an Other State Law (as applicable), it will be governed by and construed in accordance with the laws set forth in the governing law section of the Agreement. If there is any conflict between this Addendum and the DPA, the Agreement or any other data protection agreement(s) between the parties, this Addendum will prevail to the extent of that conflict with respect to the personal information of consumers only.

Attachment 3

**Compliance with the Brazilian Data Protection Law ("LGPD"),
Retroactively Effective as of September 2020**

---

1.   This Attachment 3 applies only to processing of personal data that is carried out in Brazil, that has the purpose of offering goods or services to people in Brazil, or is done on data that was collected in Brazil.

2.   Controller and Processor acknowledge that, while the text of the LGPD is available, the full details of the interpretation and enforcement of the LGDP are still being developed. In particular, regulations to be promulgated by the Brazil National Data Protection Authority (ANDP) are not final as of the date of execution of this Brazil Addendum. Controller and Processor therefore agree to attempt in good faith to comply with the LGPD in its current state and amend their respective practices and this Brazil Addendum (in accordance with the procedures set forth in Section 14(e) of the DPA) if and when required by legal developments in Brazil. Because the majority of legal obligations under the LGPD devolve upon data controllers, Controller agrees to monitor LGPD and ANDP developments and to instruct Processor whenever such developments require changes in Processor's practices or any Controller-Processor agreements.

3.   Because most legal duties and obligations under the LGPD closely track those under the GDPR, all provisions of the above DPA are incorporated and restated in this Brazil Addendum in their entirety, except as specifically amended or modified below. Without limiting the generality of this Section 3, Controller further agrees to comply with current provisions of the LGPD that may impose duties that exceed those imposed by the GDPR, including without limitation those concerning the definition of personal data and the right of data subjects to anonymization of their personal data.

4.   References to Data Privacy Laws in the DPA will mean and include (but only where applicable) LGPD.

5.   Controller and Processor acknowledge that the LGPD permits data transfers out of Brazil pursuant to Standard Contractual Clauses, but Brazil has not yet promulgated its own Standard Contractual Clause. Therefore, Controller and Processor will use the EU SCCs as specified in the DPA for such transfers, subject to the amendments and modifications stated below, until such time as Brazil promulgates Standard Contractual Clauses.

6.   Section 12 of the DPA is supplemented and amended as follows:

   (a)   Section 12(a)(iv) is amended to state: "For the purposes of clause 13 of the EU SCCs, the ANDP is the competent supervisory authority. This paragraph will constitute 'Annex I.C' for purposes of the EU SCCs."

   (b)   In Sections 12(a)(vi) and 12(a)(vii), "Ireland" is replaced by "Brazil."

   (c)   Section 12(b) of the DPA is deleted.

Attachment 4

Compliance with Argentina's Pending Data Protection Law

1.   This Attachment 4 applies only to processing of personal data of data subjects who are in Argentina that is related to the offering of goods or services to such subjects or the monitoring of their behavior within Argentina.

2.   Controller and Processor acknowledge that, as of the date of execution of this DPA, the protection of personal data in Argentina is governed by Personal Data Protection Law No. 25,326 (2000) as complemented by Regulatory Decree No. 1558/2001 and several resolutions, rules and guidelines. Controller and Processor further acknowledge that a new Data Protection Law has been introduced and is in the process of public consultation and legislative enactment (the current draft has been released as DPA Resolution 119/2022 of Sep. 12, 2022) ("ARG Pending Law")), and that its enactment is expected in 2023. Because the majority of the legal obligations under the ARG Pending Law are expected to devolve upon data controllers, Controller agrees to monitor Argentina privacy law developments and to instruct Processor whenever such developments require changes in Processor's practices or any Controller-Processor agreements.

3.   Because most legal duties and obligations under the ARG Pending Law are expected to closely track those under the GDPR, all provisions of the above DPA are incorporated and restated in this ARG Addendum in their entirety, except as specifically amended or modified below. Without limiting the generality of this Section 3, Controller further agrees to comply with any provisions of the current Personal Data Protection Law No. 25,326 (2000), as complemented, that may impose duties that exceed those imposed by the GDPR.

4.   References to Data Privacy Laws in the DPA will mean and include (but only where applicable) the current Personal Data Protection Law No. 25,326 (2000), as complemented, and (when in force) the ARG Pending Law.

5.   Controller and Processor acknowledge that the ARG Pending Law is expected to permit data transfers out of Argentina pursuant to Standard Contractual Clauses, but the specific form of such Clauses is not yet known. Therefore, Controller and Processor will use the EU SCCs as specified in the DPA for such transfers, subject to the amendments and modifications stated below, until such time as Argentina promulgates Standard Contractual Clauses.

6.   Section 12 of the DPA is supplemented and amended as follows:

(a)   Section 12(a)(iv) is amended to state: "For the purposes of clause 13 of the EU SCCs, the Argentina Agency of Access to Public Information, or any successor thereto, is the competent supervisory authority. This paragraph will constitute 'Annex I.C' for purposes of the EU SCCs."

(b)   In Sections 12(a)(vi) and 12(a)(vii), "Ireland" is replaced by "Argentina."

(c)   Section 12(b) of the DPA is deleted.

Appendix 1

CLAUSE 14(a) WARRANTY ASSESSMENT
Under Standard Contractual Clauses

Spreedly, Inc. (the "processor" or "data importer") and its customer (the "controller" or "data exporter") together provide the following assessment pursuant to Clause 14(d) of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as adopted by the European Commission on June 4, 2021 (the "EU SCCs"). The data importer and data exporter are each a "Party" and collectively the "Parties." Defined terms used but not otherwise defined in this assessment have the meanings given to such terms in the EU SCCs.

Background

Clause 14(a) of the EU SCCs requires that 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 authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses." Clauses 14(b)-(d) require that, in providing this warranty, the Parties conduct and document an assessment of the transfer in the context of the "laws and practices" of the destination country. As part of this process, "[t]he 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." This assessment is intended to be the documentation of the Parties' compliance with their obligations under Clause 14(d) and the data importer's obligation to provide relevant information under Clause 14(b).

Summary description of data importer's processing activities

The data importer hosts a web-based payments orchestration and tokenization platform which enables the controller or 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 data importer platform, and, where applicable, to automatically update expired or lost credit cards.

Assessment

The data importer is based in the United States ("U.S.") and it and its subprocessors offer services (and process personal data) in the U.S. Therefore, personal data to be processed by the data importer and its subprocessors under the Parties' agreement will be transferred to the U.S. for processing. Data importer has received legal advice on the authority of public authorities in the U.S. to access or compel disclosure of the personal data to be transferred pursuant to the Parties' agreement, with particular attention to Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 1233), as limited by President Obama's Presidential Policy Directive 28 (PPD 28). Such advice has also dealt with the practices of U.S. public authorities, to the limited extent that they are knowable. Data importer has also taken due account of the specific circumstances of the transfer, and the applicable limitations and safeguards, including technical or organizational safeguards. Of particular relevance is the fact that the personal data to be transferred consists primarily of either (1) payment card and related payment information without context into any particular transaction, or (2) basic personal data of the data exporter's personnel accessing and using data importer's software platform and services, such as the names and business contact information of such personnel.

Based on this assessment, data importer acknowledges that U.S. laws, particularly FISA, do permit U.S. public authorities to access or compel access to personal data entering the U.S., including the personal data to be transferred pursuant to the Parties' agreement. However, given the specific circumstances of the transfer and the categories and format of the transferred personal data as described above, after due consideration the data importer cannot reasonably foresee circumstances where U.S. public authorities would be likely to take interest in the personal data to be transferred pursuant to the Parties' agreement and therefore the data importer has no reason to believe such authorities are likely to exercise their authority under FISA or other similar U.S. laws to access or compel access to such personal data.