DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") applies where, and to the extent that, Spreedly, Inc. (“Processor”) processes personal data of data subjects on behalf of a customer (the “Customer”), or Customer’s customers (where relevant), 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 between Processor and Customer (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 and in the Agreement, 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 commencement of the processing of personal data pursuant to the Agreement.

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

    a. “Customer Personal Data” means any personal data processed by Processor on behalf of the Customer (or its customers) pursuant to the Agreement. For the avoidance of doubt, all Account Data (as such term is defined in the Agreement) that constitutes personal data is Customer Personal Data.

    b. “EEA” means the European Economic Area.

    c. “Data Privacy Framework” means, collectively, the terms of Processor's certification with the U.S. Department of Commerce under the EU-US Data Privacy Framework, UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework, or any substantially similar successor program recognized under Data Privacy Laws to provide for an adequate level of protection.

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

    e. “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”).

    f. “personal data” means and includes “personal information”, personally identifiable information" and “personal data” as defined under Data Privacy Laws.

    g. “Restricted Transfer” means a transfer of Customer Personal Data from the Customer to Processor or any onward transfer of Customer Personal Data from Processor to a Subprocessor, in each case where such transfer would be prohibited by Data Privacy Laws in the absence of a self-certification to the Data Privacy Framework or the parties’ agreement to the Standard Contractual Clauses or another data transfer mechanism permitted by Data Privacy laws.

    h. “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) of the Data Protection Act 2018 (referred to herein more particularly as the "UK SCCs").

i. "Subprocessor" means any person or entity (excluding employees of Processor) appointed by or on behalf of Processor to Process Customer Personal Data on behalf of the Customer (and its customers) in connection with the Agreement.

j. 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 with regard to the processing of Customer Personal Data, Customer may act either as a controller or processor and Processor acts as a processor (where Customer is a controller) or subprocessor (where Customer is a processor) under Data Privacy Laws.

3. **Customer Representations and Warranties**. The Customer represents and warrants to Processor that, prior to transferring any Customer Personal Data to Processor for processing, asking Processor to collect Customer Personal Data on the Customer's (or its customers) 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 Customer 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 Customer's behalf by Processor. The Customer 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 Customer's breach of this Section 3.

4. **Description of Processing.**

a. Data Subjects: Personnel and customers of the Customer.

b. Categories of Data: With respect to personnel of the Customer, 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 Customer, 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 Customer 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 Customer Personal Data only as needed to perform the Services and otherwise only on documented instructions from Customer (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 Customer of that legal requirement before processing (unless the applicable law prohibits

providing such information to the Customer on important grounds of public interest). The Customer will ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Customer Personal Data, and that the processing of Customer Personal Data in accordance with the Customer'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 Customer Personal Data. Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its processing of Customer 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 Customer Personal Data have committed to keeping such Customer Personal Data confidential or are under an appropriate statutory obligation of confidentiality with respect to such Customer Personal Data. Processor will take steps to ensure that any natural person acting under the authority of the Processor who has access to Customer Personal Data does not process such Customer Personal Data except as needed to perform the Services or otherwise upon instructions from the Customer, 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 Customer Personal Data appropriate to the risk, including in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed. Such measures will include, *inter alia* as appropriate: (a) the pseudonymization or encryption of Customer Personal Data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services used to process Customer Personal Data, (c) the ability to restore the availability and access to Customer 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 Customer's cost, reasonable assistance to Customer 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 Customer 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 Customer's cost, assist Customer as Customer may reasonably require, including by appropriate technical and organizational measures, insofar as this is possible, in ensuring compliance with the Customer's obligations under Data Privacy Laws to appropriately secure and safeguard Customer Personal Data (such as, where applicable, pursuant to GDPR Article 32).

    c. Taking into account the nature of the Processing, Processor will, at the Customer's cost, assist Customer as Customer may reasonably require, including by appropriate technical and organizational measures, insofar as this is possible, to enable the Customer to comply with requests by data subjects to exercise their rights under Data Privacy Laws. Processor will: (i) promptly notify the Customer if Processor receives a request from a data subject under Data Privacy Laws with respect to Customer Personal Data, and (ii) not respond to that request except on the written instructions of the Customer or as required by applicable law to which Processor is subject, in which case Processor will (to the extent permitted by applicable law) inform Customer 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 Customer 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 Customer) Processor will make such records available to the Customer upon the Customer's reasonable written request. Processor will make available to the Customer on the Customer's reasonable request all information necessary to demonstrate compliance with this DPA, and will, at the Customer's cost, allow for and cooperate with audits, including inspections, by the Customer or an auditor appointed by Customer in relation to the Processing of the Customer Personal Data by Processor, subject to the following:

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

    b. The Customer 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 Customer 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 Customer' written request to conduct an audit and/or inspection, the Processor and Customer 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 Customer with additional details of this fee including the basis of its calculation, in advance of the audit. Additionally, the Customer will be responsible for any fees charged by any third-party auditor appointed by the Customer for this audit.

    h. In lieu of an audit, upon reasonable request by the Customer, but no more than once per year, Processor agrees to complete, within thirty (30) days of receipt, an audit questionnaire provided by the Customer 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 Customer Personal Data under the Agreement without written authorization from the Customer. Processor reserves the right to maintain its Subprocessor list through means such as publication of its Subprocessor list online, and the Customer hereby provides written authorization for Processor to engage the Subprocessors listed online at https://www.spreedly.com/gdpr-subprocessors, as such list may be updated from time to time. Customer may receive notifications of new Subprocessors by emailing subprocessor@spreedly.com with the subject "Subscribe," and once subscribed in this manner Customer will receive notification of new Subprocessors

before those Subprocessors are authorized to process Customer Personal Data on behalf of the Processor. Processor will send notice to Customer by email of any additional or replacement Subprocessors at least 10 days in advance of engaging any such additional or replacement Subprocessors to process Customer Personal Data under the Agreement. Customer 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 Customer 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 Customer, and the Customer will reasonably and in good faith cooperate with Processor in such efforts. If Processor cannot resolve the Customer's objection within a reasonable period of time following receipt of Customer'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 Customer may terminate the applicable Services (such termination being without cause) 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 Customer with respect to Customer 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 Customer for the performance of that Subprocessor's obligations.

c. The Customer 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 Customer hereby consents to the transfer of Customer Personal Data to the United States for Processing by the Processor and its Subprocessors in accordance with Section 12 below.

d. Customer and Processor acknowledge that the Customer 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 Customer 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 Customer Personal Data**.

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

b. Processor (and Processor's Subprocessors) may retain Customer 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 Customer Personal Data, and will ensure that the Customer 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 Customer 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 Customer 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 Customer 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**. To the extent that Customer Personal Data includes information about individuals who are located in the EEA, the United Kingdom and/or the Swiss Confederation, and Processor or any Subprocessors store or otherwise obtain access to such Customer Personal Data outside of the EEA, the United Kingdom and/or the Swiss Confederation as a result of a Restricted Transfer, Processor hereby represents and warrants that: (i) Processor has self-certified to the Data Privacy Framework and that any such Restricted Transfers are within the scope of Processor's certification to the Data Privacy Framework; (ii) Processor will at all relevant times for purposes of this DPA maintain a "current" "current" Data Privacy Framework certification status with the United States Department of Commerce related to its processing of Customer Personal Data and remain at all times in compliance with the requirements of the Data Privacy Framework; (iii) with respect to Customer Personal Data that includes information about individuals who are located in the EEA, the United Kingdom and/or the Swiss Confederation, Processor will comply with the Data Privacy Framework principles when handling such data; (iv) Processor will promptly notify Customer if Processor makes a determination that it can no longer meet its obligations under this Section 12, and, in such event Processor will work with Customer and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any processing until such time as the processing meets the level of protection as is required by this Section 12; and (v) Processor will immediately cease (and procure that all Subprocessors immediately cease) processing such Customer Personal Data if in Customer's reasonable discretion Customer determines that Processor has not or cannot correct any non-compliance with this Section 12 in accordance with clause (iv) above within a reasonable time frame. If Customer (as "data exporter") carries out a Restricted Transfer to Processor (as "data importer") from the EEA, the United Kingdom and/or the Swiss Confederation and such Restricted Transfer is not legalized by Processor's self-certification to the Data Privacy Framework and compliance with the Data Privacy Framework principles, whether as a result of the invalidation of the Data Privacy Framework or otherwise, the parties hereby agree to apply one of the following, in descending order of preference, to the extent that a GDPR (Chapter V) data transfer mechanism or equivalent is legally required, such that the item higher in the list that is applicable and available will automatically apply during the term of this DPA and for as long as Customer Personal Data is retained by Processor: (i) an alternative suitable framework or other legally adequate transfer mechanism to which the Processor has self-certified that is recognized by the European Commission or United Kingdom Government or Swiss Government (or other relevant authority or court as applicable), as providing an adequate level of protection for personal data; (ii) any mechanism, derogation, exemption, or exception that a party is able to invoke, such as the explicit consent of the relevant data subjects, or a derogation under Article 49 of the GDPR or its equivalent under Data Privacy Laws; or (iii) the applicable 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. Where the parties agree to apply the EU SCCs with respect to a Restricted Transfer in accordance with the preceding paragraph of this Section 12, the same are incorporated by reference into this DPA on an unchanged basis save for the following:

        - Where Customer acts as a controller and Processor acts as a processor, "Module 2" (controller-to-processor) of the EU SCCs applies;
        - Where Customer's customers act as a controller, Customer acts as a processor, and Processor acts as a subprocessor, "Module 3" (processor-to-processor) of the EU SCCs applies;
        - 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;

- For the purposes of clause 11(a) of the E.U. Standard Contractual Clauses, the optional language is deleted;
- For the purposes of clause 13 of the EU SCCs: (i) if Customer 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 Customer is established, (ii) if Customer 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 Customer's representative is established, and (iii) if Customer 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 Customer 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;
- For the purposes of clause 14(a) of the EU SCCs, the Assessment attached hereto as Appendix 1 is incorporated herein by reference.
- For the purposes of clause 17 of the EU SCCs, the governing law is Ireland;
- For purposes of clause 18(b) of the EU SCCs, the selection is Ireland; and
- 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. Where the parties agree to apply the UK SCCs with respect to a Restricted Transfer in accordance with the first paragraph of this Section 12, the same are incorporated by reference into this DPA on an unchanged basis save for the following:

- In Table 2, the selections made are those that match the EU SCCs as described and detailed in clause (a) of this Section 12;
- In Table 4, both "importer" and "exporter" are selected; and
- 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.
- Nothing in the interpretation of this DPA is intended to conflict with either party's rights or responsibilities under the EU SCCs or UK SCCs (where applicable) and, in the event of such conflict, the EU SCCs (incorporating the UK SCCs where applicable) will prevail. To the extent a transfer mechanism other than the foregoing becomes reasonably available to the parties after the effective date of this DPA, the parties will consult with each other in good faith on whether to rely on such transfer mechanism in lieu of the applicable Standard Contractual Clauses.

13. **Personal Data Breach**. Taking into account the nature of processing and the information available to the Processor, Processor will reasonably assist the Customer in the Customer'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 Customer Personal Data is subject to any personal data breach Processor will, upon becoming aware of the personal data breach, without undue delay notify the Customer, take reasonable steps to contain and counteract the personal data breach and minimize any damage resulting from the personal data breach, and provide Customer with sufficient information to allow

the Customer 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 Customer's cost, to assist Customer 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 (where applicable in accordance with Section 12 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 (where applicable in accordance with Section 12), 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 46(2) 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 Customer may request reasonable changes or additions to this DPA to reflect applicable requirements. If the Customer makes a request to change or supplement this DPA pursuant to this Section 14.e, the Customer and Processor will in good faith negotiate such changes and additions (including, where applicable, providing for Customer'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. Customer 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 Customer will process using the Platform (as such term is defined in the Agreement) or that is otherwise collected by or provided to Processor or its Subprocessors under and in connection with the Services, if and to the extent Data Privacy Laws require additional clauses to be executed by Processor beyond those set forth in this DPA, then Customer 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 Customer 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.

Attachment 2

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. All capitalized terms used but not defined in this Attachment 2 will have the meanings set forth in the DPA or the Agreement.

Notwithstanding anything to the contrary elsewhere in the DPA, where the California Consumer Privacy Act of 2018 and its implementing regulations (as amended, restated or supplemented from time to time, including by the California Privacy Rights Act of 2020, the "CCPA") applies, the terms "business," "combine," "commercial purpose," "consumer," "contractor," "personal information," "processing," "sell," (and its corresponding "sale") "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");
- The Utah Consumer Privacy Act, effective December 31, 2023 (as amended, restated or supplemented from time-to-time, the "UCPA");
- The Montana Consumer Data Privacy Act, effective July 1, 2024 (as amended, restated or supplemented from time-to-time, the "MCDPA");
- The Oregon Consumer Privacy Act, effective July 1, 2024 (as amended, restated or supplemented from time-to-time, the "OCPA");
- The Texas Data Privacy and Security Act, effective July 1, 2024 (as amended, restated or supplemented from time-to-time, the "TDPSA");
- The Delaware Personal Data Privacy Act, effective January 1, 2025 (as amended, restated or supplemented from time-to-time, the "DPDPA");
- The Iowa Consumer Data Protection Act, effective January 1, 2025 (as amended, restated or supplemented from time-to-time, the "IACDPA");
- The Tennessee Information Protection Act, effective July 1, 2025 (as amended, restated or supplemented from time-to-time, the "TIPA");
- The Minnesota Consumer Data Privacy Act, effective July 31, 2025 (as amended, restated or supplemented form time-to-time, the "MNCDPA");
- The Maryland Online Data Privacy Act, effective October 1, 2025 (as amended, restated or supplemented from time-to-time, the "MODPA");
- The Indiana Consumer Data Protection Act, effective January 1, 2026 (as amended, restated or supplemented from time-to-time, the "INCDPA");
- The Rhode Island Data Transparency and Privacy Protection Act, effective January 1, 2026 (as amended, restated or supplemented from time-to-time, the "RIDPA"); and
- The Kentucky Consumer Data Protection Act, effective January 1, 2026 (as amended, restated or supplemented from time-to-time, the "KCDPA").

In consideration of the mutual obligations set forth herein, the parties agree to the terms and conditions of this Attachment 2.

1. The parties acknowledge and agree that with regard to the processing of Customer Personal Data, Customer may act either as a business or service provider and Processor acts as a service provider or contractor to the Customer under the CCPA, and Customer may act as either a controller or processor and Processor acts as a processor (where Customer is a controller) or subprocessor (where Customer is a processor) under the Other State Laws. The specific purpose for which Processor is processing personal information under the Agreement (and the only purpose for which Customer discloses personal information to Processor under this Agreement) is for Processor to provide the Platform and the Services as specifically set forth in the Agreement. Customer represents, warrants and covenants that it has complied and it will comply with the CCPA and the Other State Laws with respect to all personal information of consumers that Customer has transferred or made available to Processor and its Subprocessors, or that Customer has asked Processor or its Subprocessors to collect on Customer's behalf for processing in connection with the Services. The Customer 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 Customer's breach of this Section 1.

2. In its processing of personal information of consumers that the Customer has transferred to Processor for processing, that Processor may have access to, or that Processor has collected on the Customer's behalf, in each case in connection with the Services, Processor will comply with all requirements of the CCPA 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 Customer; (iii) not sell or (where CCPA applies) share the personal information to or with any third parties; (iv) not combine the personal information that Processor receives from, or on behalf of, Customer 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 and/or the Other State Laws, as applicable; (v) taking into account the nature of processing and the information available to Processor, by appropriate technical and organizational measures and insofar as this is reasonably practical, promptly comply with Customer's reasonable written instructions associated with responding to any consumer's request to exercise the consumer's rights under CCPA or the Other State Laws, as applicable; (vi) taking into account the nature of processing and the information available to Processor, reasonably assist Customer in meeting its obligations in relation to the security of processing personal information and in relation to providing for legally required notifications of breaches involving personal information; (vii) at Customer's direction, delete or return to Customer all personal information as requested at the end of the Agreement, unless retention of the personal information is otherwise permitted or required by law; and (viii) notify Customer after Processor makes a determination that it can no longer meet its obligations under the DPA or this Attachment 2. Customer has the right, upon notice to Processor, to take reasonable and appropriate steps to stop and remediate Processor's unauthorized use of personal information. 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 Attachment 2 will prohibit Processor from retaining, using or disclosing the personal information in connection with: (i) retaining or employing another service provider, processor, contractor or subcontractor (as applicable), provided the service provider, processor, contractor or subcontractor meets the requirements for a service provider, contractor or subcontractor under the CCPA 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 Customer, 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 Customer, accessed in connection with the Services or collected on the Customer'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 or a processor, subprocessor or subcontractor within the meaning of any applicable State Law; and (ii) requires the Subprocessor to be bound by terms that are substantially equivalent to the restrictions, duties and obligations under this Attachment 2.

5. Upon Customer's reasonable written request, and at Customer's expense, Processor will make available to Customer all information in Processor's possession necessary to demonstrate Processor's compliance with the obligations in this Attachment 2 and (solely to the extent required by applicable law) to enable Customer to conduct and document data protection assessments. Additionally, at Customer's expense, Processor will allow for, and cooperate with, reasonable

assessments by Customer or its designated assessor; alternatively, Processor may (at no additional charge to Customer) arrange for a qualified and independent assessor to conduct an assessment of Processor's policies and technical and organizational measures in support of the obligations under this Attachment 2 using an appropriate and accepted control standard or framework and assessment procedure for such assessments and provide a report of such assessment to Customer upon request. Customer acknowledges and agrees that any information, reports or assessments made available to Customer under this paragraph will be Processor's Confidential Information and will be subject to all confidentiality obligations set forth in the Agreement.

6. To the extent this Attachment 2 is not governed exclusively by CCPA 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 Attachment 2 and the DPA, the Agreement or any other data protection agreement(s) between the parties, this Attachment 2 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. Customer 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. Customer 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. Customer agrees to inform Processor if Customer becomes aware of LGPD and ANDP developments that require changes in Processor's practices or its agreements with Customer.

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, Customer 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. Customer 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, Customer 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. Customer 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. Customer 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. Customer agrees to inform Processor if Customer becomes aware of Argentina privacy law developments that require changes in Processor's practices or any its agreements with Customer.

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, Customer 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. Customer 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, Customer 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

Where the Parties (as defined below) agree to apply the EU SCCs with respect to a Restricted Transfer in accordance with Section 12 of the DPA, Spreedly, Inc. (the "data importer" and "processor") and its customer (the "data exporter" and either "controller" or "processor", the latter being the case where Customer's customers are the controller) together provide the following assessment pursuant to Clause 14(d) of 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 DPA.

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." Whilst data importer relies on the Data Privacy Framework and complies with its principles to receive data from the EEA, the United Kingdom and/or the Swiss Confederation, 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), given that data importer maintains EU SCCs as an alternative transfer mechanism in the event that the Data Privacy Framework is invalidated.

Summary description of data importer's processing activities

The data importer hosts a web-based payments orchestration and tokenization platform which enables the Customer 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. In the aftermath of the Court of Justice of the European Union ruling in CJEU - C-311/18 ("Schrems II"), the United States Government, the European Commission and the UK Government developed the Data Privacy Framework to facilitate transatlantic commerce by providing U.S. organizations with reliable mechanisms for personal data transfers to the United States from the EEA, the United Kingdom and the Swiss Confederation that are consistent with applicable Data Privacy Laws. Organizations participating in the Data Privacy Framework may receive personal data from the EEA from July 10, 2023. Organizations participating in the UK Extension to the EU-U.S. Data Privacy Framework may receive personal data from the United Kingdom and Gibraltar from October 12, 2023 when the U.S. - UK Data Bridge was approved by the UK Government. Organizations participating in the Swiss-U.S. Data Privacy Framework may receive personal data from the Swiss Confederation from September 15, 2024 when the Swiss-U.S. Data Privacy Framework was approved by the Swiss Government.

The Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities signed on October 7, 2022 set out the steps that President Biden directed the U.S. to take in order to implement its commitments to security data safety. Such directions included safeguards that limit access to data collected via U.S. surveillance activities to validated intelligence priorities in a proportional manner, requiring intelligence agencies to update their policies and procedures, accordingly, establishing an independent and impartial redress mechanism, and enhancing oversight of surveillance intelligence gathering. This Executive Order formed the basis of the European Commission and UK Government's decisions to adopt their respective findings of adequacy to ensure compliant data transfers under the Data Privacy Framework.

Whilst the entry into force of the Data Privacy Framework, and data importer, being a participant in such program and adhering to its principles alleviates the risks set out in Schrems II, data importer nonetheless considers it appropriate to address the specific U.S. laws that were discussed in the Schrems II ruling and their relevance to the use of data importer's Services as part of its warranty assessment under Clause 14(a) of the EU SCCs.

In addition to the adequacy of the Data Privacy Framework, 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.