

Data Protection Addendum

This Data Protection Addendum (“**DPA**”) is entered into as of the Effective Date (defined below) between WP Company LLC d/b/a The Washington Post (“**Post**”) and Vendor (“**Vendor**”). The Post and Vendor may each be referred to as a “**Party**” and or collectively referred to as the “**Parties**”. This DPA shall be effective on the date it has been fully executed by the Parties (the “**DPA Effective Date**”). As of the DPA Effective Date, this DPA shall be incorporated by reference into the agreement between The Post and Vendor that governs The Post’s use of the Service, whether such agreement is online or in a written agreement executed in counterparts with Vendor (“**Agreement**”). All capitalized terms used in this DPA but not defined shall have the meaning set forth in the Agreement. To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern.

1. Definitions.

“**Applicable Law**” means all applicable laws, regulations, and other legal or regulatory requirements in any jurisdiction relating to privacy, data protection/security, or the Processing of Personal Data, including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (“**CCPA**”) and the General Data Protection Regulation, Regulation (EU) 2016/679 (“**GDPR**”).

“**Personal Data Breach**” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or exfiltration of, or access to, Personal Data.

“**Personal Data**” means includes “personal data,” “personal information,” and “personally identifiable information,” and such terms shall have the same meaning as defined by Applicable Law.

“**Post Data**” means Personal Data that Vendor receives from The Post, or otherwise Processes for or on behalf of The Post, in connection with the Agreement.

“**Process**” and “**Processing**” mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Standard Contractual Clauses**” means the annex found in EU Commission Decision of 5 February 2010 *on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council* (available as of September 13, 2019 at data.europa.eu/eli/dec/2010/87/oj), completed as described in the “Data Transfers” section below.

“**Subprocessor**” means any Vendor affiliate or subcontractor engaged by Vendor for the Processing of Personal Data.

2. **Instructions to Vendor.** Vendor will retain, use, disclose, and otherwise Process the Post Data only as described in the Agreement and in compliance with The Post’s instructions, unless obligated to do otherwise by Applicable Law. In such case, Vendor will inform The Post of that legal requirement before the Processing unless legally prohibited from doing so. Without limiting the foregoing: (a) Vendor will not Process the Post Data in a manner inconsistent with Vendor’s role as The Post’s “Service Provider”, as such term is defined in the CCPA (regardless of whether the CCPA applies); (b) Vendor will not “sell” the Post Data, as such term is defined in the CCPA; and (c) Vendor hereby certifies that it understands the restrictions and obligations set forth in this DPA and that it will comply with them. The details of the Processing are set forth in the Agreement. Vendor will promptly inform The Post if, in Vendor’s opinion, an instruction from The Post infringes Applicable Law.
3. **Compliance with Law:** Vendor will comply with all Applicable Laws applicable to Vendor in its role as provider of the Services.
4. **Subprocessors.** Prior to a Subprocessor’s Processing of Personal Data, Vendor will impose contractual obligations on the Subprocessor that are substantially the same as those imposed on Vendor under this DPA. Subprocessors are listed _____. When any new Subprocessor is engaged, Vendor will provide at least 5 business days’ notice before the new Subprocessor Processes any Personal Data by adding it to the Subprocessor list, unless exigent circumstances require earlier Processing of Personal Data, in which case they will be added as soon as practicable. This paragraph constitutes The Post’s consent to the Subprocessor List, as well as any subprocessing under the Standard Contractual Clauses, if they apply. The subprocessor agreements to be provided under Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses, redacted prior to sharing with The Post, and The Post agrees that such copies will be provided by only upon request. The Post may reasonably object to Vendor’s use of a new Subprocessor by notifying Vendor promptly in writing within ten (10) business days after receipt of Vendor’s notice by _____. In its notification, The Post shall explain its reasonable grounds for objection. In the event The Post objects to a new Subprocessor, Vendor will use commercially reasonable efforts to make available to The Post a change in the Service or recommend a commercially reasonable change to The Post’s configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening The Post. If Vendor is unable to make available such change

within a reasonable period of time, which shall not exceed thirty (30) days, either Party may terminate without penalty the applicable Order Form(s) with respect only to those services which cannot be provided by Asana without the use of the objected-to new Subprocessor by providing written notice to the other Party. Vendor remains responsible for its Subprocessors and liable for their acts and omissions as for its own acts and omissions.

5. **Security.** Vendor will assist The Post in The Post's compliance with the security obligations under Applicable Law, as relevant to Vendor's role in Processing the Personal Data, taking into account the nature of Processing and the information available to Vendor, by implementing technical and organizational measures set forth in Appendix 2, without prejudice to Vendor's right to make future replacements or updates to the measures that do not lower the level of protection of Personal Data. Vendor will ensure that the persons who Vendor authorizes to Process the Personal Data are subject to a written confidentiality agreement covering such data or are under an appropriate statutory obligation of confidentiality.
6. **Personal Data Breach Notification.** Vendor will comply with the Personal Data Breach-related obligations directly applicable to it under Applicable Law. Taking into account the nature of Processing and the information available to Vendor, Vendor will assist The Post in complying with those applicable to The Post by informing The Post of a confirmed Personal Data Breach without undue delay or within the time period required by Applicable Law. Vendor will notify The Post at the [NOTIFICATION EMAIL], or at another email address that The Post provides to Vendor in writing for purposes of Personal Data Breach notifications. To the extent available, this notification will include Vendor's then-current assessment of the following, which may be based on incomplete information:
 - a. The nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned;
 - b. The likely consequences of the Personal Data Breach; and
 - c. Measures taken or proposed to be taken by Vendor to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

If requested in writing by The Post, Vendor shall notify data subjects and governmental entities or The Post customers of the Security Breach in a form reasonably acceptable to The Post (and refrain from making such notification without The Post's written consent unless required by Applicable Law).

7. **Assistance Responding to Data Subjects Requests.** To the extent legally permitted, Vendor shall promptly notify The Post if Vendor receives any requests from an individual seeking to exercise any rights afforded to them under Applicable Law regarding their Personal Data, which may include: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "Data Subject Request"). To the extent The Post, in its use of the Service, does not have the ability to address a Data Subject Request, Vendor shall, upon The Post's request, provide commercially reasonable efforts to assist The Post in responding to such Data Subject Request, to the extent Vendor is legally permitted to do so and the response to such Data Subject Request is required under Applicable Law. To the extent legally permitted, The Post shall be responsible for any costs arising from Vendor's provision of such assistance, including any fees associated with provision of additional functionality.
8. **Responding to Third-Party Requests.** If Vendor receives a request from a third party in connection with any government investigation or court proceeding that Vendor believes would require it to produce any Post Data, Vendor will inform The Post in writing of such request and cooperate with The Post if The Post wishes to limit, challenge or protect against such disclosure, to the extent permitted by Applicable Law.
9. **Assistance with DPIAs and Consultation with Supervisory Authorities.** Taking into account the nature of the Processing and the information available to Vendor, Vendor will provide reasonable assistance to and cooperation with The Post for The Post's performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving Vendor, and with related consultation with supervisory authorities, including information on the categories of The Post Data Processed and the purposes of the Processing, the use of service providers with respect to such Processing, any data disclosures or transfers to third parties and a general description of technical and organizational measures to protect the security of such data.
10. **Data Transfers.** The Post authorizes Vendor and its Subprocessors to make international transfers of the Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected. Except as provided in subsection b below, such transfer shall be subject to the Privacy Shield Framework:
 - a. Vendor has successfully certified its adherence to the EU-US or Swiss-US Privacy Shield Framework, as administered by the U.S. Department of Commerce and detailed at <https://www.privacyshield.gov> ("Privacy Shield"), and (i) Vendor's certification remains active and in effect; (ii) Vendor's certification is sufficient to cover the Personal Data; (iii) Vendor complies with the Privacy Shield with respect to the Personal Data; and (iv) under Applicable Law of the

relevant jurisdictions, the Privacy Shield remains a sufficient mechanism for addressing restrictions on the exportation of the Personal Data from such jurisdictions.

- b. Solely to the extent legally required, taking into account Vendor's Privacy Shield certification, Brexit, any obligation The Post may have under Standard Contractual Clauses that The Post concluded with third parties, and any other relevant factors, the Standard Contractual Clauses apply and take precedence over the rest of this DPA to the extent of any conflict. The Standard Contractual Clauses will be deemed completed as follows:
 - i. The "exporter" is the The Post, for itself and on behalf of its customers, and the exporter's contact information is set forth below.
 - ii. The "importer" is Vendor, and Vendor's contact information is set forth below.
 - iii. Appendices 1 and 2 of the Standard Contractual Clauses are set forth in Annex A below.
 - iv. By entering into this DPA, the Parties are deemed to be signing the Standard Contractual Clauses and its applicable Appendices.

11. **Audits:** Vendor will make readily available to The Post all information reasonably necessary to demonstrate compliance with this DPA and will allow for and contribute to audits, including inspections, conducted by The Post or another auditor designated by The Post. To the extent The Post uses a third-party representative to conduct the Audit, The Post shall ensure that such third party representative is bound by obligations of confidentiality no less protective than those contained in this Agreement. The Post shall provide Vendor with fourteen (14) days prior written notice of its intention to conduct an Audit. The Post shall conduct its Audit in a manner that will result in minimal disruption to Vendor's business operations and shall not be entitled to receive data or information of other clients of Vendor or any other Confidential Information of Vendor that is not directly relevant for the authorized purposes of the Audit.

12. **Return or Destruction:** Upon written request from The Post's authorized representative, Vendor shall delete or anonymize such Post Data in accordance with its requirements under Applicable Law. Notwithstanding the foregoing, this provision will not require Vendor to delete Post Data from archival and back-up files except as provided by Vendor's internal data deletion practices and as required by Applicable Law.

[Rest of Page Intentionally Blank / Signatures Follow]

IN WITNESS WHEREOF, the Parties by the undersigned duly authorized representatives, intending to be legally bound, have executed this Agreement as of the Effective Date.

Spreedly, Inc.		WP Company LLC	
By: <div><div>DocuSigned by:</div><div>Justin Benson</div><div>C9132818B2F844A...</div></div>		By: <div><div>DocuSigned by:</div><div>Matthew Monahan</div><div>013B0B5F72AD450...</div></div>	
Name:	Justin Benson	Name:	Matthew Monahan
Title:	CEO	Title:	Head of Product
Date:	3/6/2020	Date:	3/6/2020

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data Subjects

The personal data transferred concern the following categories of data subjects: See the Agreement for details.

Categories of Personal Data

The Personal Data Transferred concern the following categories of data: See the Agreement for details.

Special Categories of Personal Data

The personal data transferred concern the following special categories of data (please specify): None expected

Processing Operations

The personal data transferred will be subject to the following basic processing activities:

Processing for the provision of services as set forth in the underlying Agreement.

Anticipated Duration of Processing:

For the term of the Agreement, except where a different time is set forth in the Agreement.

Appendix 2 to the Standard Contractual Clauses

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 impact on the individuals to whom the Personal Data relates, Vendor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the following (among other things) as appropriate:

- a. the pseudonymization and encryption of Personal Data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c. the ability to restore the availability and access to 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.

In assessing the appropriate level of security, Vendor shall in particular take account of the risks presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Post Data. Such security measures must comply with Applicable Law.

Other than as prohibited by Applicable Law, Vendor shall immediately notify The Post of any investigations of its information use, privacy or information security practices or Personal Data Breach by a governmental, regulatory or self-regulatory organization.