

Standard Contractual Clauses Amendment

The Parties to this Standard Contractual Clauses Amendment (SCC Amendment) wish to ensure that international transfers of Personal Information are conducted in accordance with the requirements of applicable Data Protection Laws by applying the Standard Contractual Clauses as provided herein, and further wish to ensure that the Processing of Personal Information complies with applicable Data Protection Laws. This Amendment is made effective as of the last date signed by a Party (Effective Date).

1. Incorporation and Interpretation

- 1.1. This SCC Amendment amends, as applicable, any data processing addendum or similar data protection agreement(s) (the DPA) entered into by the Parties; or where no DPA exists, the Agreement.
- 1.2. Clauses 2, 3, 4, 5, 6, and 7 of this SCC Amendment are hereby incorporated into the DPA and/or Agreement. In cases where the DPA and/or the Agreement (as applicable) include provisions that relate directly to the international transfer of Personal Information to Third Countries from a Transferring Warner Media Entity established in the Restricted Countries, or Personal Information originating from Restricted Countries, (such as by requiring compliance with the U.S. Privacy Shield Program, or the predecessors to the Standard Contractual Clauses), then those provisions shall be replaced by clauses 1 to 6 of this SCC Amendment.
- 1.3. Where no active, mutually-signed Agreement exists between Vendor and Warner Media or a Warner Media Affiliate, Vendor and relevant Transferring Warner Media Entity agree that clauses 2, 3, 4, 5, and 6 of the SCC Amendment will apply to international transfers of Personal Information as set out in clause 3, 4, and 5.
- 1.4. Except as amended by this SCC Amendment, the DPA and/or Agreement will remain in full force and effect.
- 1.5. To the extent that the terms of this SCC Amendment, inclusive of the SCCs, conflict with those in the DPA and/or Agreement, the terms of this SCC Amendment shall govern. Notwithstanding the foregoing, Warner Media and Vendor agree that all liabilities between them and/or any other Transferring Warner Media Entities under the Standard Contractual Clauses will be subject to the limitations and exclusions of liability set out in the DPA and/or Agreement (as applicable), except to the extent prohibited by applicable law.

2. Definitions

For the purposes of this SCC Amendment the following terms have the same meaning as set forth in GDPR: Controller, Processor, Data Subject, Processing (with respect to Personal Information, as defined below). All other defined terms shall have the meaning given below:

“2021 SCC Relevant Transfer” means a transfer of Personal Information to a Third Country of Personal Information that is subject to GDPR, or to applicable Data Protection Law where any required legal mechanism or adequacy standard necessary to support the transfer can be met by entering into the Standard Contractual Clauses (2021).

“Affiliate” means in relation to any company, any direct or indirect subsidiary or holding company of that company or any direct or indirect subsidiary of any such holding company.

“Agreement” means the agreement or any exhibits, addenda, statements of work, work orders and similar specifications or similar entered into between Warner Media, LLC (Warner Media) or a Warner Media Affiliate and Vendor governing the provision of services and/or products by Vendor to the Warner Media and/or Warner Media Affiliates (as applicable).

“Data Protection Law” means any federal, state, provincial, local, municipal, foreign, international, multinational or other constitution, law, statute, treaty, rule, regulation, ordinance, code, and guidance issued by regulatory authorities competent to interpret or enforce the same, relating to processing Personal Data, privacy, data protection (the protection of Personal Information), or cybersecurity, as may be amended from time to time.

“Established” means the effective and real exercising of activity through stable arrangements and Establishment refers to such stable arrangement.

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

“Parties” means the parties to this SCC Amendment.

“Personal Information” means any information relating to an identified or identifiable natural person, including any information defined as “personally identifiable information,” “personal information,” “personal data” or similar terms as such terms are defined under Data Protection Laws, in each case as Processed by Vendor in connection with the services and/or products provided to Warner Media or its Affiliates.

“Restricted Country” means any country which restricts the transfer of Personal Information to another country not deemed adequate to receive such Personal Information.

“Sensitive Personal Information” means Personal Information revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; physical or mental health; sex life or sexual orientation; the Processing of genetic data, biometric data for the purpose of uniquely identifying a Data Subject; Personal Information relating to criminal convictions and offences or related security measures; and such similar subsets of Personal Information that require enhanced protections under the Data Protection Laws of the applicable Restricted Country.

“Standard Contractual Clauses” means, collectively, the Standard Contractual Clauses (2021), the Standard Contractual Clauses (2010), and the Standard Contractual Clauses (2004).

“Standard Contractual Clauses (2004)” means the alternative set of standard contractual clauses for the transfer of personal data to third countries amending Decision 2001/497/EC adopted by the European Commission decision of 27 December 2004 C(2004) 5271 available at <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF>.

“Standard Contractual Clauses (2010)” means the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC adopted by the European Commission decision of 5 February 2010 C(2010) 593, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0087>.

“Standard Contractual Clauses (2021)” means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission decision of 4 June 2021 C(2021) 3972, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

“Sub-Processor” means the person or entity which Processes Personal Information on behalf of the Processor.

“Third Country” means a country not deemed adequate to receive the Personal Information under the Data Protection Laws of the applicable Restricted Country.

“Transferred Personal Information” means any Personal Information, the transfer of which is subject to the Standard Contractual Clauses by virtue of this Amendment.

“Transferring Warner Media Entity” means Warner Media, or a Warner Media Affiliate, that transfers Personal Information it Processes to Vendor located in a Third Country.

1.3 “UK GDPR” means the GDPR as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;

1.4 “UK SCC Addendum” means the template addendum issued by the UK’s Information Commissioner’s Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18; and

1.5 “UK SCC Relevant Transfer” means a transfer to a Third Country of Personal Information that is subject to the UK GDPR.

“Vendor” means the vendor identified in the vendor signature block and any Vendor Affiliate that is party to the Agreement.

3. Application and Incorporation of the Standard Contractual Clauses (2021)

3.1. Application. Where Vendor Processes Personal Information as a Processor in a Third Country, with respect to 2021 SCC Relevant Transfers, the Standard Contractual Clauses (2021) are incorporated herein by reference and shall apply between Vendor and Warner Media Affiliate with Vendor as the data importer and the Warner Media Affiliate as the data exporter. The Standard Contractual Clauses (2021) shall constitute a separate agreement between each Warner Media Affiliate acting as a data exporter and Vendor acting as data importer.

3.2. Interpretation for Restricted Countries. Where the Restricted Country in which the exporting Warner Media Affiliate is Established, or from where the Personal Information originated, is not a member state of the EU, then: (1) references in the Standard Contractual Clauses (2021) to “EU,” “Union,” “EU Member State,” or “Member State” shall refer instead to that Restricted Country; (2) references to “Regulation (EU) 2016/679” or “that Regulation” shall refer instead to the Data Protection Laws of that Restricted Country and references to specific provisions or articles of GDPR shall be replaced with the equivalent provision or article of the Restricted Country’s Data Protection Law; (3) “supervisory authority” shall refer to the data protection authority in that Restricted Country; (4) references to the “Clauses” means this Section as it incorporates the Clauses.

3.3. Docking. For the purposes of Section I, Clause 7, the optional docking clause applies.

3.4. Controller-to-Controller Transfers. Where the Transferring Warner Media Entity and Vendor both Process the Transferred Personal Information as Controllers, Vendor agrees to comply with the obligations of a data importer as set out in the Standard Contractual Clauses (2021) which are incorporated herein by reference and construed as follows:

3.4.1. the Standard Contractual Clauses (2021) shall constitute a separate agreement between each Transferring Warner Media Entity (acting as a data exporter) and Vendor (acting as data importer); and

3.4.2. where the applicable sections of the Standard Contractual Clauses (2021) require the data exporter and the data importer to select a module, Vendor acknowledges that Module One of the Standard Contractual Clauses (2021) (*Transfer controller to controller*) shall apply.

3.5. Controller-to-Processor and Processor-to-Sub-Processor Transfers. Where Transferring Warner Media Entity Processes Personal Information as a Controller or a Processor and Vendor Processes the Transferred Personal Information as a Processor or Sub-Processor (as applicable), Vendor agrees to

comply with the obligations of a data importer, which are incorporated herein by reference and construed as follows:

- 3.5.1. The Standard Contractual Clauses (2021) shall constitute a separate agreement between each Transferring Warner Media Entity acting as a data exporter and Vendor, acting as data importer;
- 3.5.2. Where the data exporter and the data importer are directed to select a module, Vendor acknowledges that:
- 3.5.3. Module Two of the Standard Contractual Clauses (2021) (*Transfer controller to processor*) shall apply where Vendor, as data importer, is acting as the Transferring Warner Media Entity's Processor; and
- 3.5.4. Module Three of the Standard Contractual Clauses (2021) (*Transfer processor to processor*) shall apply where Vendor, as data importer, is acting as the Transferring Warner Media Entity's Sub-Processor;
- 3.5.5. For the purposes of Section II, Clause 8.1 (Modules Two and Three), the instructions to the data importer shall be instructions to Process Personal Information as necessary to perform the services and/or supply the products provided by Vendor and as may be specified in the DPA and/or Agreement; in the case of Module Three, these instructions constitute the instructions of the relevant Controller(s);
- 3.5.6. For the purposes of Section II, Clause 8.5 (Modules Two and Three), Vendor's storage, erasure and return of Personal Information, shall be construed by reference to the provisions regarding deletion and return of Personal Information in the DPA and/or Agreement. In the absence of any such provision, the Transferring Warner Media Entity agrees that Vendor may delete the Transferred Personal Information in accordance with Section II, Clause 8.5 (Module Two) and Section II, Clause 8.5 (Module Three) (as applicable); and
- 3.5.7. For the purposes of Section II, Clause 9 (Modules Two and Three), Vendor's ability to engage Sub-Processors shall be construed by reference to the provisions regarding the engaging of Sub-Processors in the DPA and/or Agreement. In the absence of any such provision, Vendor and the Transferring Warner Media Entity agree that Option 2 shall apply. Where the DPA and/or Agreement do not specify a time period for Vendor to submit requests to authorise or amend new Sub-Processors, this time period shall be thirty (30) calendar days.
- 3.6. Redress. For purposes of Section II, Clause 11, the optional language does not apply.
- 3.7. Choice of Law. For the purposes of Section IV, Clauses 17 and 18, to the extent permitted by applicable Data Protection Law, the parties agree that their respective obligations under the Standard Contractual Clauses (2021) shall be governed by the law(s) of and subject to the jurisdiction of the courts of The Netherlands.
- 3.8. Completion of Annex I, Part A. Annex I, Part A (*List of parties*) is hereby deemed to be completed with: (i) the details of the Transferring Warner Media Entity (as data exporter); and (ii) the details of Vendor (as data importer), in each case as set out in the Agreement.
- 3.9. Completion of Annex I, Part B. Annex I, Part B (*Description of the transfer*) of the Standard Contractual Clauses (2021) is hereby deemed to be completed with the information provided in Appendix 1.
- 3.10. Completion of Annex I, Part C. With respect to Annex I, Part C (*Competent Supervisory Authority*) of the Standard Contractual Clauses (2021), to the extent permitted by applicable Data Protection Law, the parties elect the data protection authority of The Netherlands. For the avoidance of doubt, the Parties

acknowledge and agree that, where the Data Protection Law of the Restricted Country governs the transfer of Personal Information, a competent supervisory authority outside the EU may be entitled to concurrent jurisdiction.

3.11. Completion of Annex II. Annex II of the Standard Contractual Clauses (2021) (*The Technical and organisational measures including technical and organisational measures to ensure the security of the data*) is hereby deemed to be completed as follows: Vendor shall implement and maintain technical and organisational security measures to adequately protect Personal Information on behalf of the Transferring Warner Media Entity against the risks inherent in the Processing of Personal Information, and risks from unauthorised or unlawful Processing, including those specified in (i) the DPA and/or the Agreement, if applicable; and (ii) Appendix 2 of this SCC Amendment.

3.12. Interpretation of Standard Contractual Clauses (2021). In the event of any inconsistency or conflict between the Standard Contractual Clauses (2021) and this Section, the provisions shall be construed in the manner that affords the greatest protections to data subjects.

4. **Applicability of the UK SCC Addendum.** Where Vendor Processes Personal Information in a Third Country, with respect to UK SCC Relevant Transfers, the UK SCC Addendum is incorporated herein by reference and shall apply between Vendor and the Transferring Warner Media Entity as follows:

4.1 Table 1 of the UK SCC Addendum is completed with the details of the Transferring Warner Media Entity (as data exporter) and the details of Vendor (as data importer), as provided in the Agreement. The “start date” is the start date, effective date, or equivalent date of the Agreement. The “key contact” for the Transferring Warner Media Entity is “Chief Privacy Officer” or that individual’s delegate who can be contacted at wmpprivacy@warnermedia.com and the “key contact” for Vendor will be communicated to the Transferring Warner Media Entity from time to time, including the contact’s specific job title and email address.

4.2 Table 2 of the UK SCC Addendum is completed by selecting “the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum”.

4.3 For the purposes of Table 2 and Table 3 of the UK SCC Addendum, the “Approved EU SCCs” are completed as set out in in sections 3.4, through 3.11 of this Addendum, as applicable.

4.4 Table 4 of the UK SCC Addendum is completed by selecting “neither party”.

4.5 In the event of any inconsistency or conflict between the UK SCC Addendum and this Section, the UK SCC Addendum shall prevail.

5. **Application and Interpretation of Standard Contractual Clauses (2010)/(2004)**

5.1. Controller to Controller Transfers. Where Vendor Processes Personal Information as a Controller in a Third Country, with respect to any transfer from a Restricted Country that is not a 2021 SCC Relevant Transfer or a UK SCC Relevant Transfer, the Standard Contractual Clauses (2004) are incorporated herein by reference and shall apply between Vendor and Warner Media Affiliate as follows:

5.1.1. The Standard Contractual Clauses (2004) shall constitute a separate agreement between each Warner Media Affiliate acting as a data exporter and Vendor acting as data importer.

5.1.2. References to “member state” shall be deemed to be references to the Restricted Country and references to Articles within Directive 95/46/EC shall be deemed to be references to the nearest equivalent provisions of the Restricted Country’s Data Protection Law.

5.1.3. For the purposes of II(h), the data importer shall process Personal Information in accordance with the principles set forth in Annex A of the Standard Contractual Clauses (2004).

5.1.4. Annex B of the Standard Contractual Clauses (2004) is completed with the information set out in Appendix 1 to this SCC Amendment.

5.2. Controller to Processor Transfers. Where Vendor Processes Personal Information as a Processor in a Third Country, with respect to any transfer from a Restricted Country that is not a 2021 SCC Relevant Transfer, the Standard Contractual Clauses (2010) are incorporated herein by reference and shall apply between Vendor and Warner Media Affiliate as follows:

5.2.1. The Standard Contractual Clauses (2010) shall constitute a separate agreement between each Warner Media Affiliate acting as a data exporter and Vendor acting as data importer.

5.2.2. References to “member state” shall be deemed to be references to the Restricted Country and references to Articles within Directive 95/46/EC shall be deemed to be references to the nearest equivalent provisions of the Restricted Country’s Data Protection Law.

5.2.3. For the purposes of Clauses 9 and 11(3) of the Standard Contractual Clauses (2010), the governing law shall be the law of the Restricted Country.

5.2.4. Appendix 1 of the Standard Contractual Clauses (2010) is completed with the information set out in Appendix 1 to this SCC Amendment.

5.2.5. Appendix 2 of the Standard Contractual Clauses (2010) is completed with the information set out in Appendix 2 to this SCC Amendment.

5.2.6. The optional illustrative indemnification shall not apply.

6. Additional Requirements for International Transfers

6.1. If Vendor at any time Processes Personal Information originating from Warner Media or a Warner Media Affiliate in any Restricted Country outside that country (including an EEA country), Vendor will, on the relevant Warner Media or Warner Media Affiliate’s instructions, take all necessary actions and execute such agreements as may be necessary under applicable data protection law in such country to legitimise any Processing or data transfer of Personal Information to Vendor and to ensure an adequate level of protection for the relevant Personal Information.

6.2. In the event that any competent authority holds that a data transfer mechanism relied on by the Parties (including pursuant to clause 5.1 above) is invalid, or any supervisory authority requires transfers of Personal Information made pursuant to such mechanism to be suspended, then the Warner Media or the relevant Warner Media Affiliate may, at its discretion, require Vendor to cease Processing Personal Information, or co-operate with it to facilitate use of an alternative transfer mechanism.

7. Additional Requirements for the Processing of Personal Information

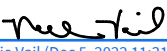
7.1. Vendor shall comply with all applicable Data Protection Law and provide the level of privacy protections required by such laws. Vendor shall notify Warner Media Affiliate at wmprivacy@warnermedia.com if it determines that it can no longer meet its obligations under Data Protection Law, and the Warner Media

Affiliate shall have the right to take appropriate steps to eliminate and remediate any such unauthorized Processing of Personal Information by Vendor.

- 7.2. Vendor shall not: (i) sell Personal Information or otherwise disclose it in exchange for monetary or other valuable consideration; (ii) Process Personal Information for any purpose other than the specific purpose of performing the Services or pursuant to the directions of the Warner Media Affiliate; (iii) Process Personal Information outside of the direct business relationship between Vendor and the Warner Media Affiliate; or (iv) combine the Personal Information with Personal Information received or collected from or on behalf of other legal or natural persons. Vendor certifies that it understands and will comply with the restrictions of this section.

IN WITNESS WHEREOF, the Parties by their duly authorized representatives, agree to the terms set forth in this SCC Amendment.

Spreedly, Inc. (Vendor) (for itself and any Vendor Affiliate that is party to the Agreement)

By: 
Nellie Vail (Dec 5, 2022 11:31 EST)


(Authorized Signature)

Name: Nellie Vail

Title: Chief Financial Officer

Date: Dec 5, 2022

Warner Media, LLC (for itself and any Warner Media Affiliate that is party to the Agreement)

By: 
Susan Rohol (Dec 9, 2022 11:03 EST)

(Authorized Signature)

Name: Susan Rohol

Title: SVP & Chief Privacy Officer

Date: Dec 9, 2022

APPENDIX 1: DETAILS OF PROCESSING

The details of the Processing of Personal Information carried out by Vendor as a Processor are as follows:

Data Subjects: Vendor will Process Personal Information relating to the following Data Subjects (check yes or no as applicable):

- ☒ employees (personnel engaged by Warner Media Affiliate)
- ☒ contractors (individuals acting in a business capacity as independent contractors to Warner Media Affiliate)
- ☐ vendors' employees/contractors (individuals acting in a business capacity who are employees of other vendors, contractors, or suppliers of Warner Media Affiliate)
- ☒ consumers or customers (individuals acting in a personal or household capacity who engage with products or services of Warner Media Affiliate, including visiting a website, creating an account, subscribing to a service, or making a purchase)
- ☐ talent (individuals acting in a professional capacity seeking a role in a production)
- ☐ job applicants (individuals seeking employment from Warner Media Affiliate, other than as talent)
- ☐ other (specify where possible): _____

Categories of Personal Information: Vendor will Process the following categories of Personal Information (check yes or no as applicable):

- ☒ personal identification (name, date of birth)
- ☐ government issued identification (driver's license, social security number, or other national identity number)
- ☒ contact details (email, phone, address)
- ☐ real-time or precise location
- ☐ education and training details
- ☐ employment-related data
- ☐ family, lifestyle, and social circumstances
- ☐ financial, economic and insurance data, including financial account numbers
- ☒ billing and payment information
- ☒ digital, device and social media identifiers or digital profiles
- ☐ account credentials
- ☐ contents of communications not directed to Vendor or Warner Media Affiliate
- ☐ any other categories of Personal Information provided by the Warner Media Affiliate to Vendor in connection with the Services (specify where possible): _____

Vendor may also Process the following Sensitive Personal Information (check yes or no as applicable):

- ☒ none
- ☐ racial or ethnic origin
- ☐ political opinions
- ☐ religious or philosophical beliefs
- ☐ trade union membership
- ☐ genetic data
- ☐ biometric data
- ☐ data concerning health (including a mental or physical health condition or diagnosis)
- ☐ sex life or sexual orientation

Frequency of Transfer: Vendor will engage in transfers of Personal Information with the following frequency:

- ☐ “One-off” (Personal Information will be transferred only on seldom, ad hoc basis.)
- ☐ Occasional (Personal Information will be transferred intermittently, but on a more predictable or frequent basis than ad hoc.)
- ☒ Ongoing/regular (Personal Information will be transferred on an ongoing or regular basis, not intermittent.)

Subject matter, nature and purpose of the Processing operations: Vendor will Process Personal Information for the purpose of providing the Services, and for such other purposes as may be described in the Agreement or instructions of the Warner Media Affiliate.

Duration of Processing (the period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period): Vendor will Process the Personal Information only for as long as Services are provided under the Agreement.

Subcontracting: Vendor has engaged the following Sub-Data Processors for Processing as of the date of the Addendum:

Name of Sub-Data Processor	Address and Country of Jurisdiction	Brief Description of Processing activities	Point of contact (name, title, contact details)
Auth0	10800 NE 8th Street Suite 700 Bellevue, WA 98004 USA	Spredly direct customer portal login	Jen Wesselhoeft, Corporate Account Manager jennifer.wesselhoeft@okta.com
AWS	410 Terry Avenue North, Seattle, WA 98109- 5210 USA	Cloud data processing	Naman Verma, Lead Cloud Data Engineer namanv@amazon.com
FiveTran	1221 Broadway Floor 20 Oakland, CA 94612 USA	SaaS data integration service	Sean Daugherty, Senior Customer Success Manager sean.daugherty@fivetrان.com
FIS/Global/Vantiv	The Walbrook Building, 25 Walbrook, London, EC4N 8AF, United Kingdom	Account updater service	William Clements, Senior Engineer William.Clements@fisglobal.com
Looker	1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Business intelligence and visualization for analytics	Emily Taylor, Engagement Manager emilytaylor@google.com
Slack	500 Howard Street San Francisco, CA 94105 USA	Private customer communication	Jude Armson, Account Manager jarmson@salesforce.com
Snowflake	Suite 3A, 106 East Babcock Street, Bozeman, Montana 59715 USA	Data warehousing	Matthew Joss, Territory Account Executive matthew.joss@snowflake.com
Zendesk	1019 Market Street San Francisco, CA 94103 USA	Inbound customer support and help center/community	Lucas Petrin, Account Manager lucas.petrin@zendesk.com

APPENDIX 2: TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE STANDARD CONTRACTUAL CLAUSES

With respect to Annex II of the Standard Contractual Clauses, Vendor shall apply the following technical and organizational measures. These safeguards are without prejudice to the measures required by the Addendum, which shall take precedence to the extent they require Vendor to implement more protective measures:

Information Security Governance	<p>A comprehensive information security program including a policy written in one or more readily accessible parts that: (1) contains technical, physical, administrative and procedural controls to provide for the security, confidentiality, integrity and availability of Personal Information and Vendor systems; (2) protect against hazards or threats and unauthorized access or use of Information; (3) controls identified risks; (4) addresses access, retention and transport of Information, and (5) acceptable use.</p> <p>Designate an individual to manage and coordinate its written security policy and who is sufficiently trained, qualified and experienced to be able to fulfill those functions and any other functions that might reasonably be expected to be carried out by the individual as a security manager or officer.</p>
Asset Management	<p>Mechanisms exist to inventory system components that: (1) Accurately reflects the current system; (2) Is at the level of granularity deemed necessary for tracking and reporting; and (3) Includes organization-defined information deemed necessary to achieve effective property accountability.</p> <p>All corporate laptops are full disk encrypted and wiped per industry standards when decommissioned.</p> <p>All infrastructure equipment housing Personal Information resides within certified third-party data centers within AWS. AWS currently uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.</p>
Business Continuity and Disaster Recovery	Plans and regular exercises to address business continuity of key people and processes along with disaster recovery plans for critical technology resiliency as well as timely restoration of access to Personal Information.
Change Management	Mechanisms exist to govern the technical configuration change control processes. Prior to implementing changes to the Spreedly platform Vendor will assess the potential impact of such changes on Security and determine whether such changes are consistent with existing Security. No changes to the Spreedly platform or Security should be made which increase the risk of a breach of Personal Information or which would reduce the controls of this Annex.
Cloud Security	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.
Compliance	Mechanisms exist to facilitate the identification and implementation of relevant legislative statutory, regulatory, and contractual controls.
Configuration Management	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.
Continuous logging and monitoring	Mechanisms exist to ensure that all systems used to store are logged, monitored, and reviewed regularly including monitoring and logging of security events, all critical assets that Process Personal Information, and system components that perform security functions for Vendor's network (e.g., firewalls, IDS/IPS, authentication servers) intended to identify actual or attempted access by unauthorized individuals and anomalous behavior by authenticated users.
Cryptographic Protections	Vendor will encrypt all Personal Information in transit and at rest, as applicable, using appropriate encryption technology. Vendor will use only strong, public encryption algorithms and reputable cryptographic implementations that meet industry best practices, are robust against cryptanalysis, are not susceptible to interference or unauthorized access, and for which key access is limited to specific authorized individuals with a need to access Personal Information in order to engage in Processing or, wherever practicable, such key access is limited solely to the exporter. Vendor will not employ any proprietary cryptography.

Pseudonymization	Wherever practicable with respect to Processing, and provided it would not interfere with Vendor's provision of the Services, pseudonymization sufficient to cause Personal Information to no longer be attributable to a specific individual, provided safeguards are in place to prevent reidentification and the algorithmic process or key to re-establish identity is held only by the data exporter
Data Classification and Handling	Mechanisms exist to facilitate the implementation of data protection controls to ensure data and assets are categorized in accordance with applicable statutory, regulatory, and contractual requirements.
Endpoint Security	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices including but not limited to (1) utilization of anti-malware technologies to detect and eradicate malicious code; (2) automatic updates of anti-malware technologies, including signature definitions; (3) ensuring that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period; and (4) utilization of host-based firewall software, or a similar technology, on all information systems, where technically feasible.
HR Security	As permitted by applicable Law, conduct reasonable background checks of any Vendor personnel that will have access to Personal Information, including Criminal Record Bureau checks. Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.
Identification and Authentication	<p>Mechanisms exist to (1) provide physical access controls, secure user authentication protocols, secure access control methods, and firewall protection; and (2) prevent terminated Vendor personnel from accessing Personal Information and Vendor systems by promptly terminating their physical and electronic access to such Personal Information.</p> <p>With respect to Vendor systems and Personal Information: (1) maintain secure control over user IDs, passwords and other authentication identifiers; (2) maintain a secure method for selecting and assigning passwords and using authentication technologies such as token devices; (3) Restrict access to only active users/accounts; (4) block user access after multiple unsuccessful attempts to login or otherwise gain access; (5) assign unique user identifications plus passwords, which are not vendor supplied default passwords; (6) require personnel to change passwords at regular intervals and whenever there is any indication of possible system or password compromise, and avoid re-using or cycling old passwords; (7) require multi-factor authentication for any remote access to Vendor systems or Personal Information.</p> <p>Duties and areas of responsibility of Vendor personnel are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Vendor system or Personal Information.</p>
Incident Response	Maintain policies and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and encouraging reporting of actual or reasonably suspected breaches of Personal Information, including: (1) training Vendor's personnel with access to Personal Information to recognize actual or potential Personal Information breaches and to escalate and notify the senior management of the foregoing; (2) mandatory post-incident review of events and actions taken concerning security of Personal Information.
Malicious Code Mitigation Software	Mechanisms exist to (1) implement and maintain software for Vendor systems that detects, protects against, removes and remedies software or computer code designed to perform an unauthorized function on, or permit unauthorized access to, an information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs; (2) run mitigation software on at least a weekly basis; (3) update mitigation software automatically, including without limitation, obtaining and implementing the most currently available virus signatures.
Network Security	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network including but not limited to (1) up-to-date firewalls between Vendor system, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks operated by Vendor that are not necessary for providing the services to customer, which are reasonably designed to maintain the security of Personal Information and Vendor system; (2) implementation and management of a secure guest network.

Physical and Environmental Security	<p>Mechanisms exist to provide (1) reasonable restrictions on physical access to Personal Information and the Spreedly platform, including the use of monitoring 24 hours /7 days a week, access controls and logs of access, and measures sufficient to prevent physical intrusions to any Vendor facility where Personal Information is Processed; and (2) physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.</p> <p>Policies concerning security for the storage, access, transportation and destruction of records and media containing Information outside of business premises.</p>
Privacy	<p>Mechanisms exist to comply with applicable privacy laws, regulations, and notices, including the implementation of a data protection program that includes elements, such as technical measures or documented procedures, to address data minimization and limited retention, data quality, and implementation of data subject rights, appropriate to the nature of the Processing and Services.</p>
Risk Management	<p>Periodic and regular information security risk assessment and monitoring of Vendor's information security program, Security and the Spreedly platform, at least annually, including: (1) identifying and assessing reasonably foreseeable internal and external threats and risks to the security, confidentiality, integrity and availability of Information; (2) assessing the likelihood of, and potential damage that can be caused by, identified threats and risks; (3) regularly testing, monitoring and evaluating the sufficiency and effectiveness of Security and Personal Information breach response actions, and documenting same; (4) assessing adequacy of Vendor personnel training concerning, and compliance with, Vendor's information security program; (5) designing, implementing, adjusting and upgrading Security in order to limit identified threats and risks, and address material changes in technology, business and sensitivity of Personal Information; and (6) assessing whether such information security program is operating in a manner reasonably calculated to prevent unauthorized access or use of Personal Information; and (6) detecting, preventing and responding to attacks, intrusions and other system failures.</p>
Secure Engineering and Architecture	<p>Mechanisms exist to facilitate the implementation of industry-recognized security and privacy practices in the specification, design, development, implementation and modification of systems and services.</p>
Security Awareness and Training	<p>Regular and periodic training of Vendor personnel concerning: (1) Security; (2) implementing Vendor's information security program; and (3) the importance of personal information security.</p>
Technology Development and Acquisition	<p>Vendor will adhere to industry best practices and standards for Secure Software Development Lifecycle (SSDLC), including all of, but not limited to, the following techniques: (1) Leveraging security guidelines from one or all the following industry best practices and standards – OWASP Top 10, SANS Top 25 and Cloud Security Alliance; (2) Consistently executed secure code reviews and testing either through manual peer review or via a code scanning solution; (3) Protection of test data and content and removal of test data and content before deployment to production; (4) System acceptance testing; and (5) System change control and approvals before deployment to production.</p>
Third Party Management	<p>Mechanisms exist to facilitate the implementation of third-party management controls including but not limited to: (1) reasonable steps and due diligence to select and retain third party vendors that are capable of maintaining security consistent with this Annex and complying with applicable legal requirements; (2) contractually requiring such vendors to maintain such security; and (3) regularly assessing and monitoring third party vendors to confirm their compliance with the applicable security required in this Annex and by law.</p>
Threat Management	<p>Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.</p>
Vulnerability and Patch Management	<p>Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information including but not limited to (1) software and firmware patching; (2) vulnerability scanning on a recurring basis; and (3) penetration testing conducted by an independent third party twice per year.</p>
Certifications and Attestations	<p>Vendor shall, at the request of data exporter, promptly provide a copy of its most recent Vendor SOC2 Type II report, PCI Attestation of Compliance and/or industry certification such as ISO/IEC 27001 or any successor standards for information security management. If Vendor does not hold such certification, it must conduct, at its own expense no less than annually, an independent third-</p>

	party audit of Vendor's security program and systems, and facilities used to Process Personal Information, with a detailed summary of the report to be provided to data exporter.
--	---











Spreadly-WarnerMedia - SCC Amendment (Final)(3491333.1)

Final Audit Report

2022-12-09

Created:	2022-12-05
By:	KB Privacy (kbprivacy@wyrick.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAATP4JbR-Sly97ff4U6P4AkiW_XQtQdUPN

"Spreadly-WarnerMedia - SCC Amendment (Final)(3491333.1)" History

-  Document created by KB Privacy (kbprivacy@wyrick.com)
2022-12-05 - 2:49:50 PM GMT
-  Document emailed to Rachel Ruffing (rruffing@spreadly.com) for signature
2022-12-05 - 2:51:21 PM GMT
-  Email viewed by Rachel Ruffing (rruffing@spreadly.com)
2022-12-05 - 2:54:15 PM GMT
-  Document signing delegated to Nellie Vail (Nellie@spreadly.com) by Rachel Ruffing (rruffing@spreadly.com)
2022-12-05 - 2:56:04 PM GMT
-  Document emailed to Nellie Vail (Nellie@spreadly.com) for signature
2022-12-05 - 2:56:05 PM GMT
-  Email viewed by Nellie Vail (Nellie@spreadly.com)
2022-12-05 - 4:30:55 PM GMT
-  Document e-signed by Nellie Vail (Nellie@spreadly.com)
Signature Date: 2022-12-05 - 4:31:16 PM GMT - Time Source: server
-  Document emailed to Susan Rohol (susan.rohol@warnerbros.com) for signature
2022-12-05 - 4:31:17 PM GMT
-  Email viewed by Susan Rohol (susan.rohol@warnerbros.com)
2022-12-05 - 6:37:03 PM GMT
-  Document e-signed by Susan Rohol (susan.rohol@warnerbros.com)
Signature Date: 2022-12-09 - 4:03:07 PM GMT - Time Source: server

✔ Agreement completed.

2022-12-09 - 4:03:07 PM GMT