SPROUT SOCIAL, INC.

DATA PROCESSING ADDENDUM

Revised November 18, 2022

This Data Processing Addendum ("**DPA**") forms part of the Agreement (as defined herein) between Sprout Social,Inc. ("**Sprout Social**") and the entity entering the Agreement as a subscriber of any Sprout Social's services ("**Subscriber**").

This DPA is incorporated into, and supplemental to, the Agreement and sets out the roles and obligations that apply when Sprout Social processes Subscriber Personal Data (as defined herein) on behalf of Subscriber in the course of providing the Sprout Social products and services ("Services").

All capitalized terms not defined in this DPA shall have the same meanings set forth in the Agreement.

1. DEFINITIONS

1.1 For the purposes of this DPA:

(a) "**Applicable Data Protection Law**" means all United States Data Protection Laws and European Data Protection Laws.

(b) "**Agreement**" means the applicable Sprout Social Terms of Service, Sprout Social Service Subscription Agreement, or other written or electronic agreement executed by and between Sprout Social and Subscriber governing Subscriber's access and use of the Services.

(c) "**AWS**" means Amazon Web Services.

(d) "**EEA**" means the European Economic Area.

(e) "**European Data Protection Laws**" means as applicable to each respective party and their processing of Subscriber Data under this DPA: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**EU GDPR**"); (ii) the Switzerland Federal Act on Data Protection of 19 June 1992 (SR 235.1) and its subsequent revisions ("**FADP**"); and (iii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), or (iii); in each case as may be amended or superseded from time to time.

(f) "**Independent Auditor**" means an independent third-party auditor designated by Subscriber and approved by Sprout Social.

(g) "**Personal Data**" means any information that is protected as "personal data", "personal information", or the like under the Applicable Data Protection Laws, unless such definition does not exist, in which case it shall mean "personal data" as defined under the EU GDPR.

(h) "**Personnel**" means Sprout Social employees, vendors, and agents who have access to Personal Data.

(i) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination

by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data fromthe United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the FADP applies, a transfer of personal data from Switzerland to any other country which is not subject to legislation that guarantees adequate protection and/or is not recognized as providing an adequate level of data protection by the Swiss Federal Data Protection and Information Commissioner.

(j) "**Security Incident**" means any breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure, use, modification or access of Subscriber Personal Data processed by Sprout Social. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Subscriber Personal Data, including but not limited to unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

(k) "**Standard Contractual Clauses**" or "**EU SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personaldata to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(l) "**Sub-processor**" means any third-party Processor authorized by Sprout Social to process Subscriber Personal Data.

(m) "**Subscriber Personal Data**" means Personal Data processed by Sprout Social on behalf of a Subscriber pursuant to or in connection with the Agreement, as described in **Annex 1** of this DPA.

(n) The terms "**Business**", "**Business Purpose**", "**Consumer**", "**Contractor**," "**Controller**", "**data subject**", "**personal data**", "**personal information**", "**Processor**", "**processing**", "**sell**", "**share**" "**Service Provider**", "**special categories of data**", "**Sensitive Personal Information**", and "**Third Party**" have the meanings given to them under Applicable Data Protection Law.

(o) "**UK Addendum**" means the UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018.

(p) "**United States Data Protection Laws**" means all data protection or privacy laws and regulations in force within the United States and that are directly applicable to a party and its respective processing of Subscriber Personal Data under this DPA, including, but not limited to, the California Consumer Privacy Act and its amendments ("**CCPA**"), the California Privacy Rights Act of 2020 ("**CPRA**") and any rules or regulations implementing the foregoing.

2. ROLES AND RESPONSIBILITIES

2.1 Scope. This DPA applies only to Subscriber Personal Data that is subject to Applicable Data Protection Law by Sprout Social in its capacity as a Processor (or Service Provider) for the purpose of providing the Services. The subject matter, duration, nature and purposes of processing, and the types of Personal Data and categories of data subjects are described in **Annex 1** of this DPA.

2.2 Roles of the Parties. With respect to the processing of Subscriber Personal Data (including any Subscriber Personal Data accessed via integrations with Third Party Services) and for the purposes of Applicable Data Protection Laws, Subscriber is the Controller (or Business, as applicable) and Sprout

Social is the Subscriber's Processor (or Service Provider, as applicable).

2.3 Subscriber's Obligations. Subscriber shall: (a) comply with its obligations as a Controller (or Business) under all applicable laws relating to privacy and data protection in respect of its use of the Services and any processing instructions it issues to Sprout Social; (b) have sole responsibility for the accuracy, legality, and quality of Subscriber Personal Data; (c) ensure that Subscriber has the right to transfer, or provide access to, Subscriber Personal Data to Sprout Social for processing pursuant to the Agreement and this DPA; and (d) use commercially reasonable efforts to not disclose (nor permit any data subject to disclose) any Sensitive Information (as defined in the Agreement), Sensitive Personal Information, or special categories of data to Sprout Social for processing.

2.4 Sprout Social's Obligations. Sprout Social shall process Subscriber Personal Data only for the purposes described in the Agreement and in accordance with the lawful, documented instructions of Subscriber (including the instructions of any users accessing the Services on Subscriber's behalf) as set out in the Agreement, this DPA or otherwise in writing. Except where required by Applicable Data Protection Laws, Sprout Social shall not: (a) sell or share the Subscriber Personal Data except as explicitly instructed by Subscriber; (b) retain, use, or disclose Subscriber Personal Data for any purpose other than for the specific purpose of performing the Services in accordance with the Agreement and this DPA; (c) retain, use, or disclose the Subscriber Personal Data for a commercial purpose other than providing the Services; (d) retain, use, or disclose the Subscriber Personal Data outside ofthe direct business relationship between Sprout Social and Subscriber; or (e) combine Subscriber Personal Data with Personal Data that it receives from, or on behalf of, another person or persons, or collects from Sprout Social's own interaction with the Consumer; provided that Sprout Social may combine Personal Data to perform any business purpose, as defined in the CPRA. Sprout Social certifies that it understands these restrictions and will comply with them.

2.5 Remediation. Subscriber may take reasonable and appropriate steps to ensure that Sprout Social uses the Subscriber Personal Data that it received from, or on behalf of, the Subscriber in a manner consistent with the Subscriber's obligations under the Applicable Data Protection Laws. Subscriber also has the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Subscriber Personal Data; provided such steps shall not interfere with Sprout Social's regular business operations, shall not require Sprout Social to disclose any trade secrets or confidential information of Sprout Social, its customers or its service providers, contractors or third parties, and that Subscriber shall bear all related expenses, including any expenses related to business interruptions or other indirect expenses.

3. SECURITY

3.1 Security Measures. Sprout Social shall implement and maintain appropriate technical and organizational measures designed to protect Subscriber Personal Data from a Security Incident and to preserve the security, confidentiality, and integrity of Subscriber Personal Data, as further described in **Annex II** of this DPA. Sprout Social may update or modify its security measures from time to time, provided that such updates or modifications do not materially decrease the overall security of the Services provided to Subscriber.

3.2 Confidentiality Obligations. Sprout Social shall ensure that any personnel that it authorizes to process the Subscriber Personal Data shall be subject to a duty of confidentiality.

3.3 Security Incidents. Sprout Social shall: (a) notify Subscriber without undue delay after becoming aware of a Security Incident; (b) take commercially reasonable steps to assist in the investigation, mitigation, and remediation of such Security Incident; and (c) provide reasonable information and cooperation to Subscriber so that Subscriber can fulfill any Security Incident reporting obligations it

may have under Applicable Data Protection Laws. Notwithstanding the foregoing, to the extent permitted under applicable law, Sprout Social will not disclose any information: (i) that it deems a trade secret, (ii) that is confidential or proprietary in nature, or (iii) over which it intends to assert attorney-client privilege or any similar privilege or protection. Sprout Social shall not identify Subscriber in any public disclosure regarding a Security Incident involving Subscriber Personal Data without Subscriber's prior written consent; provided that Sprout Social may publicly acknowledge or disclose the occurrence of a Security Incident in a manner that does not identify Subscriber.

4. SUB-PROCESSING

4.1 Sub-processors. Subscriber agrees that Sprout Social may engage Sub-processors; provided that:

(a) Sprout Social shall maintain an up-to-date list of Sub-processors available at https://sproutsocial.com/subprocessors/ which it shall update with details of any new Sub-processors at least ten (10) days prior to any such change and shall notify Subscriber in advance of such new Sub-processor processing Subscriber Personal Data;

(b) Sprout Social shall impose on such Sub-processors data protection terms that require the Sub-processor to protect the Subscriber Personal Data to the standard required by Applicable Data Protection Laws;

(c) The copies of the Sub-processor agreements that must be provided by Sprout Social to Subscriber pursuant to Clause 9(c) of the EU SCCs may have all commercial information, or clauses unrelated to the EU SCCs or their equivalent, removed by Sprout Social beforehand; and, that such copies will be provided by Sprout Social, in a manner to be determined in its discretion, only upon request by Subscriber;

(d) Sprout Social remains liable for any breach of the DPA caused by a Sub-processor; and

(e) All such Sub-processors shall be Service Providers or Contractors, as applicable, for purposes of United States Data Protection Laws.

4.2 Objection to Sub-processors. Subscriber may object prior to Sprout Social's appointment or replacement of a Sub-processor provided such objection is based on reasonable grounds relating to data protection. In such event, the parties shall cooperate in good faith to reach a resolution and if such resolution cannot be reached, then Sprout Social, at its discretion, will either not appoint or replace the Sub-processor or, will permit Subscriber to suspend or terminate the affected Service and provide Subscriber with a pro-rated refund of any prepaid unused fees under the Agreement.

5. INTERNATIONAL TRANSFERS

5.1 Restricted Transfers. The parties agree that when the transfer of Subscriber Personal Data from Subscriber to Sprout Social is a Restricted Transfer and European Data Protection Laws require that appropriate safeguards are put in place, such transfers shall be subject to Standard Contractual Clauses, which shall be deemed incorporated by reference and form an integral part of this DPA as described in this Section.

5.2 EU GDPR Transfers. In relation to Restricted Transfers of Subscriber Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(a) Module Two will apply;
(b) in Clause 7, the optional docking clause will not apply;

(c) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 4.1(a) of this DPA;
(d) in Clause 11, the optional language will not apply;
(e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
(f) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
(g) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA; and
(h) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA.

5.3 FADP Transfers. In relation to Restricted Transfers of Subscriber Personal Data that is protected by the FADP, the EU SCCs will apply completed as provided in Section 5.2 above, with the following changes:

(a) references to "Regulation (EU) 2016/679" shall be interpreted as references to the FADP;
(b) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section the FADP;
(c) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", or "Swiss law";
(d) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (*i.e.*, Switzerland);
(e) in Clause 17, Option 1 will apply, and the EU SCCs shall be governed by the laws of Switzerland; and
(f) with respect to transfers to which the FADP applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

5.4 UK GDPR Transfers. In relation to Restricted Transfers of Subscriber Personal Data that is protected by the UK GDPR:

(a) the EU SCCs shall apply as completed in accordance with Section 5.2 above and shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the parties and incorporated into and form an integral part of this DPA; and
(b) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information set out in Annex I and Annex II of this DPA and the options "neither party" shall be deemed checked in Table 4.

6. COOPERATION AND DATA SUBJECT RIGHTS

6.1 Data subject and consumer rights. Sprout Social shall provide reasonable assistance to Subscriber, at Subscriber's expense, to enable Subscriber to respond to requests from data subjects and/or Consumers seeking to exercise their rights under Applicable Data Protection Law. Sprout Social shall promptly inform Subscriber in the event such request is made directly to Sprout Social. Subscriber authorizes Sprout Social to respond to requests from data subjects or Consumers seeking to exercise their rights under Applicable Data Protection Law to clarify and/or re-direct requests to Subscriber or third-party service providers, including to inform data subjects or Consumers that Sprout Social is the Processor/Service Provider acting on behalf of a Controller/Business, including naming Subscriber as the Controller/Business.

6.2 Data protection impact assessments. Taking into account the nature of the processing and the information available to Sprout Social, Sprout Social shall provide reasonable assistance needed to

fulfil Subscriber's obligation under Applicable Data Protection Law to carry out data protection impact assessments and prior consultations with supervisory authorities; provided that Sprout Social shall not be liable for any failure of Subscriber to comply with Subscriber's own obligations under Applicable Data Protection Law. Sprout Social will make available, at Subscriber's expense, all information reasonably required by Subscriber to illustrate compliance with the Applicable Data Protection Laws.

7. AUDITS

7.1 Standards Audits. Sprout Social will be assessed against industry security frameworks or standards including, but not limited to, SOC 2 standards. Upon request and no more than once per calendar year, Sprout Social shall provide Subscriber a summary copy of Sprout Social's most recent certified audit report to Subscriber; provided that such report shall be subject to the confidentiality terms under the Agreement.

7.2 Compliance Audits. Upon Subscriber's reasonable request, and no more than once per calendar year, Sprout Social will make available for Subscriber's inspection and audit, copies of certifications, records or reports demonstrating Sprout Social's compliance with this DPA. In the event that Subscriber reasonably determines that it must inspect Sprout Social's premises or equipment for the purposes of this DPA, then no more than once per calendar year, Subscriber may conduct such audit at Subscriber's expense through an Independent Auditor. Before the commencement of any such on-site inspection, Subscriber and Sprout Social shall mutually agree on reasonable timing, scope, and security controls applicable to the audit (including without limitation restricting access to Sprout Social's trade secrets and data belonging to Sprout Social's other customers). Any inspection will be of reasonable duration, will not unreasonably interfere with Sprout Social's day-to-day operations, and will be limited in scope to Sprout Social's Processing of Subscriber Personal Data.

7.3 Independent Auditors. All Independent Auditors are required to enter into a non-disclosure agreement containing confidentiality provisions reasonably acceptable to Sprout Social and intended to protect Sprout Social's and its customers' confidential and proprietary information. Subscriber will make (and ensure that any Independent Auditor makes) reasonable endeavors to avoid causing any damage, injury or disruption to Sprout Social's premises, equipment, personnel and business in the course of such an audit. Subscriber will be solely responsible for any and all costs arising from or related to any damage, injury, or disruption to Sprout Social's premises, equipment, personnel, or business caused by an Independent Auditor in the course of such audit.

8. DATA RETENTION AND DELETION

8.1 Data Retention. Unless otherwise instructed by Subscriber, Sprout Social may retain Subscriber Personal Data for up to thirteen (13) months after termination of the Agreement for the purposes of future account reactivation. Any confidentiality obligations and use restrictions in the Agreement and this DPA will continue to apply to such Subscriber Personal Data for the duration of retention.

8.2 Data Deletion and Return. Subject to Section 8.1, Sprout Social shall (at Subscriber's election) delete or return to Subscriber the Subscriber Personal Data in Sprout Social's possession upon Subscriber's written request at the termination or expiry of the Agreement. The parties agree that the certification of deletion of Personal Data that is described in Clause 16(d) of the EU SCCs shall be provided by Sprout Social to Subscriber only upon Subscriber's request. Notwithstanding the foregoing, Sprout Social may retain copies of such Subscriber Personal Data as necessary to comply with applicable law or Sprout Social's data retention policy.

9. MISCELLANEOUS

9.1 Incorporation. This DPA is incorporated into and forms part of the Agreement. Except as amended by this DPA, the Agreement will remain in full force and effect. For matters not addressed under this DPA, the terms of the Agreement apply.

9.2 Conflicts. If there is a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will control to the extent necessary to resolve the conflict.

9.3 Governing Law. This DPA shall be governed by, and construed in accordance with, the laws of the jurisdiction stipulated in the Agreement and the courts the jurisdiction stipulated in the Agreement shall have exclusive jurisdiction to hear any dispute or other issue arising out of, or in connection with, this DPA, except where otherwise required by Applicable Data Protection law or by the jurisdictional provisions set forth in the applicable Standard Contractual Clauses.

9.4 Modifications. Subscriber agrees that Sprout Social may modify this DPA at any time provided Sprout Social may only modify the Standard Contractual Clauses (a) to incorporate any new version of the Standard Contractual Clauses (or similar model clauses) that may be adopted under European Data Protection Law or (b) to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency. If Sprout Social makes any material modifications to this DPA, Sprout Social shall provide Subscriber with at least ten (10) days' notice (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect by either: (a) sending an email to the email address of the designated account owner in Subscriber's Services account; or (b) alerting Subscriber via the user interface. If Subscriber reasonably objects to any such change, Subscriber may terminate the Agreement by giving written notice to Sprout Social within ten (10) days of notice from Sprout Social of the change.

The parties' authorized signatories have duly executed this DPA.

[SIGNATURE PAGE FOLLOWS]

Subscriber

Signature: _____

Subscriber Legal Name:

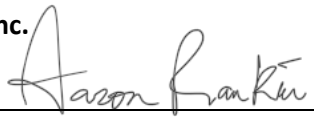
_____

Print Name: _____

Title: _____

Date: _____

Sprout Social, Inc.

Signature: 

Print Name: Aaron Rankin

Title: Chief Technology Officer

Annex I
Data Processing Description

This Annex I forms part of the DPA and describes the processing that the Sprout Social will perform on behalf of the Subscriber. Capitalized terms in Annex I shall have the meaning assigned to them in the Agreement and DPA.

1. LIST OF PARTIES

Controller(s) / Data exporter(s):

Name:	Each of the Subscriber entities identified in the Agreement.
Address:	The addresses of each of the Subscriber entities identified in the Agreement.
Contact person's name, position and contact details:	Data protection enquiries can be addressed to [Subscriber to insert]
Activities relevant to the data transferred under the SCCs:	Receipt of the Services
Signature and date:	This Annex I shall be deemed executed upon execution of the DPA.
Role (controller/processor):	Controller

Processor(s) / Data importer(s):

Name:	Sprout Social, Inc.
Address:	131 S. Dearborn St. Suite 700 Chicago, IL 60603
Contact person's name, position and contact details:	Data protection enquiries can be addressed to privacy@sproutsocial.com
Activities relevant to the data transferred under the SCCs:	Provision of the Services
Signature and date:	This Annex I shall be deemed executed upon execution of the DPA.
Role (controller/processor):	Processor

2. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Sprout Social core platform: The Personal Data processed concerns users of the Services (typically, employees or contractors of Subscriber authorized to use the Services) and individual social media users who interact with the social media accounts, which are owned and/or operated by Subscriber Sprout Social employee advocacy tool: The Personal Data processed concerns employee advocacy users (typically employees of Subscriber) who interact with the employee advocacy tool and share content that is uploaded and posted by Subscriber

Categories of personal data transferred:	Sprout Social core platform: Account user data (name, business email address, IP address, and language preference), social media profile data (the specific types of personal data collected are dependent on each social network, but typically include username, profile picture, and first/last name if provided), geographic location, usage, social media content (*e.g.* posts, comments, pages, profiles, likes, feeds) and engagement and analytics metrics, including social media metadata (*e.g.* number of social media followers, number of posts, number of tweets). Sprout Social employee advocacy tool: account user data (name, business email address, IP address, and language preference), social media profile data of account users (the specific types of personal data that is collected is dependent on each social network, but typically includes username, profile photo, and first and last name if provided), social media engagement and analytics metrics (number of posts, public engagements, and number of clicks on posts published through Subscriber's employee advocacy service) NOTE: The Sprout Social employee advocacy tool does not collect any Personal Data on Sprout Social employee advocacy tool users' first and second degree connections on the social networks. The only information collected on first and second degree connections is aggregated engagement data.
Sensitive data transferred (if applicable) and applied restrictions or safeguards thatfully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access onlyfor staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfersor additional security measures:	Sprout Social does not intentionally collect or transfer any sensitive data in relation to these data subjects and does not require this data to operate the Services.
The frequency of the transfer (*e.g.* whether the data is transferred on a one- off or continuous basis):	Continuous for the duration of the Agreement.
Nature of the processing:	Collection, storage, organization, modification, retrieval, disclosure, communication, and other uses in the performance of the Services as set out in the Agreement.

Purpose(s) of the data transfer and further processing:	Processing to perform the Services as set out in the Agreement, including as described below: Sprout Social core platform: Personal Data will be processed to provide social media-related engagement, publishing, analytics, listening, and monitoring software services to the Subscriber in accordance with the Agreement. These services will consist of providing platform and performance analytics to the Subscriber in relation to connected social media profiles. Full details about Sprout Social's social media management tool can be found at https://sproutsocial. com/ Sprout Social employee advocacy tool: Personal Data will be processed by Sprout Social to provide the Sprout Social employee advocacy tool to Subscriber in accordance with the Agreement. The Sprout Social employee advocacy tool will consist of providing a sharing platform to the Subscriber for its employees to share curated content on their connected social media profiles.
The period for which the personal data willbe retained, or, if that is not possible, the criteria used to determine that period:	Personal Data will be retained in accordance with Section 8 of the DPA.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Processing activities in performance of the Services, as set out in the Agreement, including providing access to the Services. Personal Data will be retained in accordance with Section 8 of DPA.

3. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (*e.g.* in accordance with Clause 13 EU SCCs)	Where the EU GDPR applies, the competent supervisory authority shall be determined in accordance with Clause 13 of the EU SCCs. Where the UK GDPR applies, the competent supervisory authority shall be the UK Information Commissioner's Office. Where the FADP applies, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

ANNEX II

Security Standards

This Annex II forms part of the DPA and describes the security standards and practices utilized by Sprout Social in providing the Services to Subscriber. Capitalized terms in Annex II shall have the same meaning assigned to them in the Agreement and DPA.

1. SECURITY MEASURES

1.1 Information Security Policies. Sprout Social maintains information security policies that are reviewed at least annually and revised whenever material changes are made to the systems or procedures that access or utilize Subscriber Personal Data. All employees must affirm their responsibilities in protecting Subscriber Personal Data set forth in such policies as a condition of employment.

1.2 Identity and Access Management. Access to Subscriber Personal Data is granted under the principle of least privilege. Only authorized Personnel have access to Subscriber Personal Data. Sprout Social restricts access to the production environments to designated Sprout Social employees based on documented permissions as defined in a role-based user access matrix.

1.3 Authentication. Access to Sprout Social systems, tools, services, and endpoints are subject to password standards in conjunction with multi-factor authentication or integration into our central identity provider, which also enforces multi-factor authentication.

1.4 Encryption At Rest and In Transit. All Subscriber Personal Data, including backups, are encrypted at rest using the AES-256 specification. All communications over public networks with Sprout Social's application and API utilize TLS 1.2 or greater.

1.5 Vulnerability Management. Sprout Social regularly scans systems and applications that contain Subscriber Personal Data for common vulnerabilities. Sprout Social conducts application security code analysis to ensure that the Services are not vulnerable to known attacks and remediates high-severity issues in a reasonable timeframe.

1.6 Penetration Testing. Sprout Social contracts with reputable penetration testing vendors to conduct penetration testing no less than once per year.

1.7 Intrusion Detection System (IDS). Sprout Social utilizes an intrusion detection system to detect, evaluate, and respond to security threats and unusual system activity. Alerts are sent to security Personnel who are available to respond on a 24/7 basis.

1.8 Data Center and Physical Security. The Services are hosted by AWS in world-class hosting facilities that are secure, highly available, and redundant. More information regarding AWS's data center and physical security standards can be found at https://aws.amazon.com/compliance/data-center/controls/.

1.9 Disaster Recovery and Backups. Sprout Social maintains a disaster recovery and business continuity plan which is reviewed and updated at least annually. Backups are taken frequently, encrypted in transit and at rest, and are tested regularly.

2. PERSONNEL AND SUB-PROCESSOR SECURITY

2.1 Personnel Security. Sprout Social ensures that all Personnel take appropriate security measures to maintain the confidentiality, integrity, and availability of personal data. Sprout Social maintains protocols designed to ensure that Personnel follow established security policies. Sprout Social employs appropriate technical and organizational measures to ensure Personnel conduct themselves

in accordance with established company guidelines and policies. Disciplinary procedures are applied if Personnel fail to adhere to relevant policies.

2.2 Employee Screening and Security. Sprout Social screens prospective employees, and conducts background checks where permitted by law, before employment and the conditions of employment are applied. Sprout Social maintains an employee handbook, a code of conduct, and an acceptable use policy to convey controls and values to employees, including sanctions for non-compliance. Sprout Social provides its employees with semi-annual security and privacy training.

2.3 Sub-processor Security. Before engagement, all Sub-processors must go through an internal vendor review and approval process which includes review by Sprout Social's security, legal, privacy, and finance teams. The Sprout Social security team performs due diligence of our Sub-processors on an annual basis to ensure continued compliance with information security controls.

3. APPLICATION SECURITY FEATURES

3.1 Multi-factor Authentication. The Services support multi-factor authentication (MFA) apps that implement the Time-based One-time Password (TOTP) algorithm for generating passcodes.

3.2 Single Sign On. The Services support single sign-on (SSO) with identity providers that support the SAML 2.0 standard.

3.3 Secure Credentials. Sprout Social account passwords are salted and hashed using industry-standard algorithms.

4. SECURITY INCIDENTS

4.1 Security Incident Policies. Sprout Social maintains an incident response plan, an incident handling and notification policy, and other supporting procedures based on NIST standards. These policies ensure consistent classification, documentation, response, and notification for Security Incidents in accordance with Sprout Social's commitment to data privacy and security.

5. COMPLIANCE AND CERTIFICATIONS

5.1 Service Organization Control Compliance. Sprout Social undergoes a SOC 2 Type 2 audit annually which is performed by an independent third-party auditor. A copy of Sprout Social's most recent SOC 2 report is available upon request to Subscribers who are parties to an Agreement with Sprout Social or who agree to hold the report in confidence under a Sprout Social non-disclosure agreement. Additional information on Sprout Social's certifications can be found at https://sproutsocial.com/trustcenter/.

5.2 Data Center Certifications. The Services are hosted on AWS which is compliant with Cloud Security Alliance Star Level 2, ISO 9001, 27001, 27017, 27018, 27701, 22301, PCI DSS Level 1, and SOC 1, 2, and 3 standards. More information on compliance and certifications at AWS can be found at https://aws.amazon.com/compliance/.