SPROUT SOCIAL, INC.
DATA PROCESSING ADDENDUM

Revised October 2020

This Data Processing Addendum **("DPA")** forms part of the Agreement between Sprout Social, Inc. and its affiliates **("Sprout Social")** and the entity entering the Agreement as a customer of Sprout Social's Services **("Customer").**

This DPA is supplemental to the Agreement and sets out the roles and obligations that apply when Sprout Social processes Personal Data falling within the scope of the GDPR or Personal Information falling within the scope of the CCPA on behalf of Customer in the course of providing the Sprout Social Services.

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

1. Definitions

1.1 For the purposes of this DPA:

(a) **"Agreement"** means the terms and conditions or other written or electronic agreement between Sprout Social and Customer setting out the provision and use of the Sprout Social Services.

(b) **"CCPA"** means the California Consumer Privacy Act.

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

(d) **"GDPR"** means 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, and repealing Directive 95/46/EC.

(e) **"Standard Contractual Clauses"** means Annex 2, attached to and forming part of this DPA pursuant to the European 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.

(l) The terms **"Controller", "Processor", "Personal Data", "processing", "special categories of data"** and **"data subject"** have the meanings given to them in the GDPR.

(g) The terms **"Business", "Service Provider", "Third Party", "Personal Information", "Consumer", "sell",** and **"Business Purposes"** have the meanings given to them in the CCPA.

2. Applicability of DPA

To the extent that Sprout Social processes Personal Data falling within the scope of the GDPR on behalf of Customer in the course of providing the Sprout Social Services, the relevant provisions of this DPA apply. To the extent that Sprout Social processes Personal Information falling within the scope of the CCPA on behalf of Customer in the course of providing the Sprout Social Services, the relevant provisions of this DPA apply. For the avoidance of doubt, where it is not clear whether the GDPR, the CCPA, or both apply, all provisions of this DPA shall apply.

3. Roles and Responsibilities

3.1 Roles of the Parties. As between Sprout Social and Customer, Customer is the Data Controller for purposes of the GDPR of the Personal Data, and the Business for purposes of the CCPA with respect to the Personal Information, that is provided to Sprout Social for processing under the Agreement and as described in Appendix 1 and Sprout Social shall process the Personal Data and/or Personal Information as a Data Processor and/or Services Provider on behalf of Customer.

3.2 Customer Processing of Personal Data/Personal Information. Customer shall be responsible for:

(a) Complying with all applicable laws relating to privacy and data protection in respect of its use of the Sprout Social Services, its processing of the Personal Data and/or Personal Information, and any processing instructions it issues to Sprout Social;

(b) Ensuring it has the right to transfer, or provide access to, the Personal Data and/or Personal Information to Sprout Social for processing pursuant to the Agreement and this DPA; and

(c) Ensuring that it shall not disclose (nor permit any data subject to disclose) any special categories of data to Sprout Social for processing.

3.3 Sprout Social's processing of Personal Data/Personal Information. Sprout Social shall process the Personal Data and/or Personal Information only for the purposes described in the Agreement and in accordance with the lawful, documented instructions of Customer (including the instructions of any users accessing the Sprout Social Services on Customer's behalf) as set out in the Agreement, this DPA or otherwise in writing. Sprout Social shall not: (a) sell the Personal Data or Personal Information; (b) retain, use, or disclose the Personal Data or Personal Information for any purpose other than for the specific purpose of performing the Sprout Social Services; (c) retain, use, or disclose the Personal Data or Personal Information for a commercial purpose other than providing the Sprout Social Services; or (d) retain, use, or disclose the information outside of the direct business relationship between Sprout Social and the Customer. Sprout Social certifies that it understands these restrictions and will comply with them.

4. Security

4.1 Security. Sprout Social shall implement appropriate technical and organizational measures to protect the Personal Data and/or Personal Information from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (a **"Security Incident").**

4.2 Confidentiality Obligations. Sprout Social shall ensure that any personnel that it authorizes to process the Personal Data and/or Personal Information shall be subject to a duty of confidentiality.

4.3 Security Incidents. Upon becoming aware of a Security Incident, Sprout Social shall notify Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfill any data breach reporting obligations it may have under the GDPR or other applicable laws.

4.4 Appropriate Use of Products and Services. Customer agrees that, without prejudice to Sprout Social's obligations under this DPA, (i) Customer is solely responsible for its use of Sprout Social's products and services, including (a) making appropriate use of the products and services to ensure a level of security appropriate to the risk in respect of Customer Personal Data/Personal Information; and (b) securing the account authentication credentials, systems and devices Customer uses to access the products or services; and (ii) Sprout Social has no obligation to protect Customer Personal Data/Personal Information that Customer elects to store or transfer outside of Sprout Social's and/or its sub- processors' systems.

5. Sub-processing

5.1 Sub-processors. Customer agrees that Sprout Social may engage Sprout Social affiliates and third party sub-processors **("Sub-processors")** to process Personal Data and/or Personal Information on Sprout Social's behalf provided that:

(a) Sprout Social shall maintain an up to date list of Sub-processors which it shall update with details of any change in Sub-processors at least five (5) days prior to any such change and shall notify Customer in advance of such change;

(b) Sprout Social imposes on such Sub-processors data protection terms that require it to protect the Personal Data and/or Personal Information to the standard required by applicable data protection laws; and

(c) The copies of the Sub-processor agreements that must be provided by Sprout Social to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses 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 Customer.

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

(e) All such Sub-processors shall be Service Providers for purposes of the CCPA.

5.2 Objection to Sub-processors. Customer 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 Customer to suspend or terminate the affected Sprout Social Service (without prejudice to any fees incurred by Customer prior to suspension or termination).

6. International Transfers

Standard Contractual Clauses. The Standard Contractual Clauses, attached hereto as Annex A, will apply to Customer Data that is transferred outside the EEA or the United Kingdom, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data. The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA or the United Kingdom. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if Sprout Social has adopted, at its sole discretion, Binding Corporate Rules for Processors or an alternative, recognized compliance standard for the lawful transfer of Personal Data outside the EEA or the United Kingdom.

7. Cooperation and Audits

7.1 Data subject and consumer rights. Sprout Social shall provide reasonable assistance to

Customer, insofar as this is possible and at Customer's expense, to enable Customer to respond to requests from data subjects and/or consumers seeking to exercise their rights under the GDPR or the CCPA. In the event such request is made directly to Sprout Social, Sprout Social shall promptly inform Customer of the same. Customer authorizes Sprout Social to respond to requests from data subjects/or Consumers seeking to exercise their rights under the GDPR or the CCPA in order to clarify requests.

7.2 Data protection impact assessments. Sprout Social shall, taking into account the nature of the processing and the information available to it, provide reasonable assistance needed to fulfil Customer's obligation under the GDPR to carry out data protection impact assessments and prior consultations with supervisory authorities, provided, however, that Sprout Social shall not be liable for any failure of Customer to comply with Customer's own obligations related thereto.

Sprout Social will be assessed against industry security frameworks or standards including, but not limited to, SOC 2 standards. Upon request, Sprout Social shall provide a summary copy of its most recent certified audit report to Customer, which reports shall be subject to Sprout Social's confidentiality terms under the Agreement.

7.3 Audits. Upon Customer's reasonable request, and no more than once per calendar year, Sprout Social will make available for Customer's inspection and audit, copies of certifications, records or reports demonstrating Sprout Social's compliance with this DPA. In the event that Customer reasonably determines that it must inspect Sprout Social's premises or equipment for purposes of this DPA, then no more than once per calendar year, any audits described in this Section 7.3 will be conducted, at Customer's expense, through an independent third-party auditor ("Independent Auditor") designated by Customer. Before the commencement of any such on-site inspection, Customer 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 and will not unreasonably interfere with Sprout Social's day-to-day operations. 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. Customer 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 or inspection. To the extent that Customer or any Independent Auditor causes any damage, injury or disruption to the Sprout Social's premises, equipment, personnel and business in the course of such an audit or inspection, Customer will be solely responsible for any costs associatedtherewith.

8. Return/Deletion of Data

Return or deletion of Personal Data. Upon request by Customer at the termination of the Agreement, Sprout Social shall delete or return to Customer the Customer's Personal Data and/or Personal Information in Sprout Social's possession, except to the extent such data may be required to be retained by Sprout Social under applicable laws or Sprout Social's data retention policies adopted in accordance with such laws, including on backup systems; provided, however, the confidentiality obligations and use restrictions in the Agreement will continue to apply to such Customer Personal Data for the duration of retention. Customer acknowledges that notwithstanding the foregoing language of this section, Sprout Social retains Customer Personal Data for up to thirteen (13) months after the termination of any Agreement for the purposes of future account reactivation. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Sprout Social to Customer only upon Customer's request.

9. Liability

Each party’s liability to the other taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations on liability set forth in the Agreement. Sprout Social’s total liability for all claims from the Customer arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement.

10. Miscellaneous

10.1 Except as amended by this DPA, the Agreement will remain in full force and effect.

10.2 Any claims brought under this DPA shall be subject to the Agreement, including but not limited to the exclusions and limitations of liability set forth in the Agreement.

10.3 This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, if there is a conflict between this DPA and the Agreement, the DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

10.4 This DPA shall be governed by, and construed in accordance with, the laws of the State of Illinois and the courts of Cook County, Illinois 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.

10.5 Customer agrees that Sprout Social may modify this DPA at any time provided Sprout Social may only modify the Standard Contractual Clauses in Annex A (i) to incorporate any new version of the Standard Contractual Clauses (or similar model clauses) that may be adopted under GDPR or (ii) 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 Customer 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 Customer’s Sprout Social Services account; or (b) alerting Customer via the user interface. If Customer reasonably objects to any such change, Customer 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.

Customer

Signature: ______________________________

Customer Legal Name:

____

Print Name: _______________________________

Title: ________________________________

Date: ________________________________

Sprout Social, Inc.

Signature: Aaron Rankin

Print Name: Aaron Rankin

Title: Chief Technology Officer

ANNEX A

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.:___________; fax:__________________; e-mail: __________________

Other information needed to identify the organisation

…………………………………………………………

(the data **exporter**)

And

Name of the data importing organisation: Sprout Social, Inc.

Address: 131 S. Dearborn St., Suite 700, Chicago, IL 60603

Tel.: (866) 878-3231; e-mail: privacy@sproutsocial.com

Other information needed to identify the organisation:

………………………………………………………………

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of

Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

On behalf of the data importer:

Name (written out in full): Aaron Rankin

Position: Chief Technology Officer

Address: 131 S. Dearborn St., Suite 700, Chicago, IL 60603

Other information necessary in order for the contract to be binding (if any):

Signature……Aaron Rankin……………………………….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is:

Data importer
The data importer is: Sprout Social

Data subjects
The personal data transferred concern the following categories of data subjects:
Other data subjects:

Sprout Social: The personal data and personal information processed concern individuals who interact with connected social media accounts, which are owned and/or operated by Customer

Bambu: The personal data and personal information processed concern Bambu users (typically employees of Customer) who interact with the Bambu platform and share content that is uploaded and posted by Customer

Simply Measured: The personal data and personal information processed concern individuals who interact with connected social media accounts, which are owned and/or operated by the Customer.

Other data subjects:

Categories of data
The personal data transferred concern the following categories of data:

Sprout Social: customer & third-party social media profile information including temporary authorization tokens for any linked accounts on social media networks; geographic location; usage; social media content; social media performance

Bambu: social media profile information including temporary authorization tokens for any linked accounts on social media networks; social media content; social media performance

Simply Measured: geographic location; type of device used; social media profile information including temporary authorization tokens for any linked accounts on social media networks; usage

Other categories of data:

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

Customer does not intentionally collect or transfer any sensitive personal data in relation to these data subjects

Other categories of special data:

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

Sprout Social:

- *Personal data and personal information will be transferred from the Customer to Sprout Social to provide social media-related engagement, publishing, analytics, listening, and monitoring software services to the Customer*

- *These services will consist of providing a platform and performance analytics to the Customer in relation to connected social media profiles*

- *Full details about Sprout Social's social media management tool can be found at https://sproutsocial. com/*

Bambu:

- *Personal data and personal information will be transferred from the Customer to Sprout Social for Sprout Social to provide its Bambu platform to Customer.*
- *These services will consist of providing a sharing platform to the Customer for its employees to share curated content on their connected social media profiles.*

Simply Measured:

- *Personal data and personal information will be transferred from the Customer to Simply Measured for Simply Measured to provide social media-related engagement, publishing and analytics services on behalf of the Customer.*
- *These services will consist of providing a platform and performance analytics to the Customer in relation to connected social media profiles.*
- *Full details about Simply Measured's products and services can be found at https://simplymeasured. com.*

Other processing activities:

DATA EXPORTER

Name:

Authorised Signature ……………………

DATA IMPORTER

Name: Aaron Rankin

Authorised Signature Aaron Rankin ……………………

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The Security Standards described in Annex B to this GDPR Addendum for Processors

ANNEX B

Security Standards

These terms form part of the Data Processing Addendum for Vendors and, if applicable, the Standard Contractual Clauses between Company and Vendor.

1. Personnel Security

Sprout Social employs appropriate technical and organizational measures to ensure personnel, subcontractors, vendors, and agents who have access to Personal Data and/or Personal Information ("Personnel") conduct themselves in accordance with established company guidelines and policies. Sprout Social maintains an Employee Handbook, which includes a Code of Conduct and Acceptable Use Policy, to convey these controls and values to employees, including sanctions for non-compliance, and employees receive semi-annual security and privacy training. Prospective employees are screened, including, where permitted by law, background checks, before employment and the conditions of employment are applied. Sprout Social has put in place protocols designed to ensure that Personnel strictly follow established security policies and procedures. Disciplinary process is applied if Personnel fail to adhere to relevant policies and procedures.

2. Information Security Program

Sprout Social's Information Security Program shall include specific security requirements aligned to industry-recognized best practices, measured by a commitment to SOC 2 Type 2 controls, ensuring the highest quality processes are in place. The Information Security Program includes, but is not limited to, the following areas:

a. Information Security Policies and Standards: Sprout Social maintains information security policies, standards, and procedures which are reviewed at least annually and revised whenever material changes are made to the systems or procedures that access or utilize Personal Data.

b. Identity and Access Management: Access to data is granted under the principle of least privilege. Only authorized Sprout Social personnel, in service of the given customer, have access to customer data. Sprout Social restricts access to the production environments to designated personnel based on documented permissions as defined in a user access matrix.

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

d. Security Incident Response: Sprout Social maintains an Incident Response Plan, an Incident Handling and Notification Policy, and other supporting procedures to ensure consistent classification, documentation, response, and notification for security incidents. These step-by-step procedures help ensure the Security and Legal teams, in conjunction with Sprout Social management or other stakeholders, handle such incidents with consistency and in accordance with our commitment to data privacy and data protection.

3. Application Security & Accessibility

Sprout Social uses industry-recognized best practices to maintain secure and accessible services.

a. Data Storage: Sprout Social leverages a third-party cloud hosted Infrastructure-as-a-Service (“IaaS”). Data stores containing customer information are co-mingled but logically separated and encrypted-at-rest.

b. Transmission: Data is encrypted when transmitted over public networks. User authentication information and the transmission of private or confidential information to the Sprout Social application is encrypted-in-transit using TLS.

c. Data Backup/Restoration: Systems are designed for resiliency, durability, and availability within the IaaS. Backups of data stores occur daily across multiple locations. Server and infrastructure configuration is stored in version control, as is our software code. In the event of a disaster, systems will be restored from these sources.

d. Penetration Testing: Sprout Social contracts with penetration testing vendors to perform external penetration testing of the Sprout Social application.

e. Bug Bounty Program: A public bug bounty program is maintained and submissions are reviewed by the Sprout Social Security team, escalated to the appropriate engineering team, and tracked to resolution

f. Intrusion Detection System (IDS): Sprout Social utilizes IDS to detect, evaluate, and respond to security threats and unusual system activity. Alerts sent to Infrastructure and Security personnel are monitored 24/7.

4. Sub-Processor Security

Before engagement, new sub-processors go through an internal vendor review and approval process which includes the Security, Legal, and Finance teams. Once assessed, the sub-processors are required to enter into appropriate contractual agreements outlining security, confidentiality, and availability. The Security team performs due diligence of our sub-processors and critical third-party vendors on an annual basis to ensure compliance with service-level agreements, contractual obligations, and information security controls.