SPROUT SOCIAL, INC.
DATA PROCESSING ADDENDUM

Revised September 27, 2021

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 EU/UK Data Protection Law or Personal Information falling within the scope of the CCPA on behalf of Customer in the course of providing the Sprout Social services ("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) "EU/UK Data Protection Law" means: (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) (the "EU GDPR"); and (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); in each case as may be amended or superseded from time to time.

(e) "Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the 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.

(f) "Standard Contractual Clauses" means: (i) where the EU GDPR applies, 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 personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs").

(g) The terms "Controller", "Processor", "Personal Data", "processing", "special categories of data" and "data subject" have the meanings given to them in the EU GDPR and UK GDPR.
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 EU/UK Data Protection Law 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 EU/UK Data Protection Law, 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 Controller for purposes of EU/UK Data Protection Law 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 Annex 1 and Sprout Social shall process the Personal Data and/or Personal Information as a Processor and/or Service 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 Information; (b) retain, use, or disclose Personal Information for any purpose other than for the specific purpose of performing the Sprout Social Services; (c) retain, use, or disclose the 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
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 EU/UK Data Protection Law 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 the Personal Data and/or 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 the Personal Data and/or 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 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 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**

6.1 The parties agree that when the transfer of Personal Data from Customer to Sprout Social is a Restricted Transfer, it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:
Module Two will apply;

in Clause 7, the optional docking clause will not apply;

in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 5.1(a) of this Agreement;

in Clause 11, the optional language will not apply;

in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

in Clause 18(b), disputes shall be resolved before the courts of Ireland;

Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Agreement;

Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Agreement; and

in relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(i) For so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of personal data to processors set out in the European Commission’s Decision 2010/87/EU of 5 February 2010 (“Prior C2P SCCs”) for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between the Customer and Sprout Social on the following basis:

(A) Appendix 1 shall be completed with the relevant information set out in Annex I to this Agreement;

(B) Appendix 2 shall be completed with the relevant information set out in Annex II to this Agreement; and

(C) the optional illustrative indemnification Clause will not apply.

(ii) Where sub-clause (b)(i) above does not apply, but the Customer and Sprout Social are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a “UK Addendum to the EU Standard Contractual Clauses” (“UK Addendum”) issued by the Information Commissioner’s Office under s.119A(1) of the Data Protection Act 2018, then:

(A) the EU SCCs, completed as set out in this Agreement shall also apply to transfers of such Personal Data, subject to sub-clause (B) below;

(B) the UK Addendum shall be deemed executed between the Customer and Sprout Social, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data.

(iii) If neither sub-clause (b)(i) or sub-clause (b)(ii) applies, then Customer and Sprout Social shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK GDPR without undue delay.

in the event that any provision of this Agreement contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
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 EU/UK Data Protection Law 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 EU/UK Data Protection Law 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 EU/UK Data Protection Law 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 associated therewith.

8. Return/Deletion of Data

Return or deletion of Personal Data. Sprout Social retains the Personal Data and/or Personal Information for up to thirteen (13) months after the termination of any Agreement for the purposes of future account reactivation. Any confidentiality obligations and use restrictions in the Agreement will continue to apply to such Personal Data and/or Personal Information for the duration of retention. Notwithstanding the foregoing, upon request by Customer at the termination of the Agreement, Sprout Social shall delete or return to Customer the 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. 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 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 EU/UK Data Protection Law 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.

[SIGNATURE PAGE FOLLOWS]
Customer
Signature: __________________________

Customer 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 Customer.

A. LIST OF PARTIES
Controller(s) / Data exporter(s):

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Name: Each of the Customer entities identified in the Agreement. Address: The addresses of each of the Customer entities identified in the Agreement. Contact person's name, position and contact details: Data protection enquiries can be addressed to [Customer 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</td>
</tr>
</tbody>
</table>

Processor(s) / Data importer(s):

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>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 <a href="mailto:privacy@sproutsocial.com">privacy@sproutsocial.com</a> 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</td>
</tr>
</tbody>
</table>

B. DESCRIPTION OF TRANSFER

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of data subjects whose personal data is transferred: Sprout Social: The personal data and personal information processed concerns users of the Services (typically, employees or contractors of Customer) and individual social media users who interact with connected social media accounts, which are owned and/or operated by Customer Bambu: The personal data and personal information processed concerns Bambu users (typically employees of Customer) who interact with the Bambu platform and share content that is uploaded and posted by Customer</td>
<td></td>
</tr>
<tr>
<td>Categories of personal data transferred: Sprout Social: account user data (name, business email address, IP address, and language preference), social media profile data (the specific types of personal data</td>
<td></td>
</tr>
<tr>
<td><strong>Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:</strong></td>
<td><strong>Customer does not intentionally collect or transfer any sensitive personal data in relation to these data subjects.</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):</strong></td>
<td><strong>Continuous for the duration of the Agreement.</strong></td>
</tr>
<tr>
<td><strong>Nature of the processing:</strong></td>
<td><strong>Provision of the Services.</strong></td>
</tr>
</tbody>
</table>
| **Purpose(s) of the data transfer and further processing:** | **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 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 and engagement and analytics metrics

Bambu: 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 Customer’s Bambu service)

**NOTE:** The Bambu product does not collect any personal information on Bambu users’ first and second degree connections on the social networks. The only information collected on first and second degree connections is aggregated engagement data.
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.

<table>
<thead>
<tr>
<th>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:</th>
<th>Sprout Social will retain the Personal Data for the duration of the Agreement. Upon termination of the Agreement, it will be deleted in accordance with this DPA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:</td>
<td>See Section 5 of the DPA.</td>
</tr>
</tbody>
</table>

**C. COMPETENT SUPERVISORY AUTHORITY**

<table>
<thead>
<tr>
<th>Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 EU SCCs)</th>
<th>Where the EU GDPR applies, the competent supervisory authority shall be the Irish Data Protection Commissioner. Where the UK GDPR applies, the competent supervisory authority shall be the UK Information Commissioner's Office.</th>
</tr>
</thead>
</table>
ANNEX II

Security Standards

These standards form part of the DPA and, if applicable, the Standard Contractual Clauses between Customer and Sprout Social.

They describe the technical and organisational measures implemented by Sprout Social to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

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 and/or Personal Information.

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

• 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.

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

• 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

• Intrusion Detection System (IDS): Sprout Social utilizes an 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 their commitment to confidentiality, integrity, 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.