Data Protection Addendum

In the course of providing the SparkPost service to our customers, SparkPost may process personal data on our customer's behalf where such personal data is subject to EU data protection laws like GDPR. To this end, we offer a data protection addendum (DPA) as provided below. The DPA will only be legally binding and effective if: (1) it is executed here; and (2) you are SparkPost customer on the date it is fully executed. Please note that because we have so many customers, we are not able to change the DPA for any particular customer. However, if you have any questions about the DPA, please contact us at privacy@sparkpost.com.

1. DEFINITIONS.
    1. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
    2. **"Agreement**" means the Terms of Use and the related Order, which together govern the provision and use of the Service.
    3. "**CCPA**" means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time.
    4. **"Controller/Processor Standard Contractual Clauses"** means the "Controller to Processor" (Module 2) modules of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to GDPR and the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
    5. "**Data Protection Laws**" means all laws and regulations of any jurisdiction applicable to the confidentiality, privacy, security, or Processing of Personal Data under the Agreement, including, where applicable, the GDPR, the CCPA and all other laws and regulations relating to privacy, direct marketing or data protection.
    6. "**Data Controller**" means an entity, alone or jointly with others, that determines the purposes and means of the Processing of Personal Data.

7. “**Data Processor**” means an entity that Processes Personal Data on behalf of a Data Controller.
8. “**Data Subject**” means the individual to whom Personal Data relates.
9. “**Data Subject Request**” means a Data Subject’s request to exercise that person’s rights under Data Protection Laws in respect of that person’s Personal Data, including, without limitation, the right to access, correct, amend, transfer, obtain a copy of, object to the processing of, block, delete, or opt out of the sale of such Personal Data.
10. “**EEA**” means the European Economic Area and Switzerland.
11. “**GDPR**” means either (i) the 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); or (ii) solely with respect to the United Kingdom, the Data Protection Act 2018.
12. “**Personal Data**” means any information that identifies, relates to, describes, or is reasonably capable of being associated with an identified or identifiable natural person or household.
13. “**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
14. “**Processor/Sub-Processor Standard Contractual Clauses**” means the “Processor to Processor” (Module 3) modules of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to GDPR and the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
15. “**Regulator**” means the European data protection authority or other regulatory, governmental or supervisory authority with authority over all or any part of (a) the provision or receipt of the Service; (b) the Processing of Personal Data in connection with the Service; or (c) SparkPost’s business or personnel relating to the Service.
16. “**Security Incident**” means any accidental, unauthorized or unlawful destruction, loss, alteration, disclosure of, access to, or encryption of Personal Data.
17. “**Service**” means any product or service provided by SparkPost to Customer pursuant to the Agreement.
18. “**EEA Standard Contractual Clauses**” means either (i) the Controller/Processor Standard Contractual Clauses; or (ii) the Processor/Sub-processor Standard Contractual Clauses, either individually or collectively, as applicable.
19. “**Sub-processor**” means the entity which Processes Personal Data on behalf of an entity acting as a Processor or a Sub-processor.
20. “**UK Standard Contractual Clauses**” means the standard contractual clauses for the transfer of personal data to processors established in third countries in the form set out by European Commission Decision 2010/87/EU, as may be amended, modified or superseded by the European Commission.

2. RELATIONSHIP WITH THE AGREEMENT.

1. The parties agree that this DPA will replace any existing data protection addendum or similar agreement the parties may have previously entered into in connection with the Services.
2. This DPA applies where and only to the extent that SparkPost Processes Personal Data that is subject to Data Protection Laws in the course of providing the Service pursuant to the Agreement.
3. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between the terms of this DPA and the terms of the Agreement, this DPA will prevail to the extent of that conflict. In circumstances where SparkPost is relying on the EEA Standard Contractual Clauses or UK Standard Contractual Clauses (collectively, "**Standard Contractual Clauses**"), as applicable, to transfer Personal Data, the applicable Standard Contractual Clauses shall prevail in the event of a conflict with this DPA.
4. Any claims brought under or in connection with this DPA will be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.
5. The parties agree that no limitations of liability set out in the Agreement will apply to any party's liability to Data Subjects under the third-party beneficiary provisions of the Standard Contractual Clauses to the extent limitation of such liability is prohibited by Data Protection Laws.
6. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.
7. This DPA shall remain in effect so long as SparkPost Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

3. ROLES AND SCOPE OF PROCESSING.
    1. **Role of the Parties**. The parties acknowledge and agree that, as between SparkPost and Customer:
        1. With respect to the Personal Data of any individual accessing and/or using the Service through the Customer's Account ("**Users**"), Customer is the Controller and SparkPost is the Processor of User Personal Data; and
        2. with respect to the Personal Data any individual: (i) whose email address is included in the Customer's recipient list(s); (ii) whose information is stored on or collected via the Service, or (ii) to whom Users send emails or otherwise engage or communicate with via the Service (collectively, "**Recipients**"), Customer is the Processor and SparkPost is the Sub-processor of Recipients Personal Data.
    2. **Customer Processing of Personal Data**. Customer agrees that it will comply with its obligations under applicable Data Protection Laws in respect of its Processing of Personal Data in connection with the Service and in respect of any documented Processing instructions it issues to SparkPost.
    3. **SparkPost Processing of Personal Data**. Customer instructs SparkPost to Process Personal Data in accordance with the Agreement (including, for the avoidance of doubt, to perform its other obligations and exercise its rights under the Agreement) and to comply with Customer's other reasonable instructions (e.g., via email) where such instructions are consistent with the Agreement. SparkPost shall:

(i) Process Personal Data only on Customer's behalf and in accordance with Customer's documented lawful instructions and shall treat Personal Data as confidential information subject to the confidentiality provisions of the Agreement; (ii) notify Customer in writing immediately if, in SparkPost's reasonable opinion, SparkPost believes that any instruction given by Customer infringes Data Protection Laws; (iii) perform the Service and Process Personal Data in compliance with Data Protection Laws and the Agreement; (iv) promptly notify Customer of any noncompliance with this DPA. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to SparkPost in relation to the processing of Personal Data and processing outside the scope of these instructions (if any) will require prior written agreement between Customer and SparkPost.

4. **Details of Data Processing**.
    1. *Subject matter:* The subject matter of the data processing under this DPA is the Personal Data.
    2. *Duration:* As between SparkPost and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.
    3. *Purpose:* The purpose of the data processing under this DPA is the provision of the Service to the Customer and the performance of SparkPost pursuant to the Agreement (including this DPA) or as otherwise agreed by the parties.
    4. *Nature of the processing:* SparkPost provides an email delivery, analytics, and intelligence service and other related services, as described in the Agreement.
    5. *Categories of data subjects*: Users and Recipients.
    6. *Types of Personal Data:*
        1. Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (account details, payment information); employment details (employer, job title, geographic location, area of responsibility);
        2. Recipients: identification and contact data (name, email address, and other demographic and segment data provided by Customer); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data).
5. **California Consumer Privacy Act**. SparkPost will comply with the CCPA and treat all Personal Data subject to the CCPA ("**CCPA Personal Data**") in accordance with the provisions of the CCPA. With respect to CCPA Personal Data, SparkPost is a service provider under the CCPA. SparkPost will not (a) sell CCPA Personal Data; (b) retain, use or disclose any CCPA Personal Data for any purpose other than for the specific purpose of providing the Services, including retaining, using or disclosing CCPA Personal Data for a commercial purpose other than providing the Services; or (c) retain, use or disclose CCPA Personal Data outside of the direct business relationship between SparkPost and Customer. The parties acknowledge and agree that the Processing of CCPA Personal Data authorized by Customer's instructions described in the Agreement and this DPA is integral to and encompassed by SparkPost's provision of the Services and the direct business relationship between the parties. The parties acknowledge and agree that SparkPost access to Customer

Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement. To the extent that any Usage Data is considered CCPA Personal Data, SparkPost is the business with respect to such data and will Process such data in accordance with its Privacy Policy, which can be found at https://www.sparkpost.com/policies/privacy/. The terms “business”, “commercial purpose”, “service provider”, and “sell” as used in this Section have the meanings given to them in the CCPA. SparkPost and Customer certify that they understand and will comply with the obligations and restrictions set forth in this DPA and the Agreement as required under the CCPA.

6. **Legitimate Interests**. Customer acknowledges that SparkPost will have a right to use and disclose data relating to the operation, support and/or use of the Service for its legitimate business purposes, such as billing, account management, technical support, and product development. To the extent any such data is considered Personal Data under Data Protection Laws, SparkPost is the Data Controller of such data and accordingly will process such data in accordance with the SparkPost Privacy Policy and Data Protection Laws.
7. **Tracking Technologies**. Customer acknowledges that in connection with the performance of the Service, SparkPost employs the use of web beacons, tracking pixels, and similar tracking technologies (“**Tracking Technologies**”). Customer will maintain an appropriate lawful basis of processing as required by Data Protection Laws to enable SparkPost to deploy Tracking Technologies lawfully on, and collect data from, the devices of Recipients in accordance with and as described in the SparkPost Privacy Policy.

4. SUBPROCESSING.
    1. **Authorized Sub-processors**. Customer agrees that SparkPost may engage Sub-processors to process Customer Data on Customer’s behalf. the Sub-processors engaged by SparkPost and authorized by Customer as of the Effective Date are listed at: https://www.sparkpost.com/policies/subprocessors.
    2. **Sub-processor Obligations**. SparkPost will: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause SparkPost to breach any of its obligations under this DPA.
    3. **Notification**. SparkPost will (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email will suffice) if it adds a Sub-processors at least ten (10) days prior to any such changes.
    4. **Objection**. Customer may object in writing to SparkPost’s appointment of a new Sub-processor within five (5) days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If a resolution is not achieved within a reasonable amount of time, Customer may terminate the applicable Order(s) in respect only to the specific Service that cannot be provided by SparkPost without the use of the objected-to new Sub-processor, by providing written notice to SparkPost.

5. SECURITY.
    1. **Security Policy**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, SparkPost shall implement and maintain appropriate technical and organizational security measures to protect Personal Data from Security Incidents and to preserve the security, integrity, availability, resiliency and confidentiality of the Personal Data and SparkPost systems used for Processing Personal Data.
    2. **Updates to Security Measures**. Customer is responsible for reviewing the information made available by SparkPost relating to data security and making an independent determination as to whether such information meets Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Policy is subject to technical progress and development and that SparkPost may update or modify the Security Policy from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service purchased by the Customer.
    3. **Customer Responsibilities**. Notwithstanding the above, Customer agrees that Customer is responsible for securing its Account authentication credentials in Customer's custody or control and protecting the security of Personal Data when in transit to and from the Service to the extent such Personal Data is in Customer's custody or control.
    4. **SparkPost Personnel**. SparkPost shall ensure that its personnel engaged in Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements in respect of the Personal Data that survive termination of the personnel engagement.
6. AUDIT REPORT AND AUDITS.
    1. **Audit Report**. SparkPost is regularly audited against the SOC 2 Type II controls (or equivalent) by independent third party auditors. Upon request, SparkPost will supply a summary copy of its audit report(s) ("**Audit Report**") to Customer, so that Customer can verify SparkPost's compliance with the audit standards against which it has been assessed, and this DPA. Such Audit Reports, as well as any conclusions or findings specified therein, are SparkPost's Confidential Information.
    2. **Audit**. SparkPost will make available to Customer all information necessary to demonstrate compliance with the obligations of Data Processors laid down in Article 28 of GDPR ("**Article 28 Requirements**"). To this end, SparkPost will provide written responses to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm SparkPost's compliance with Article 28 Requirements, provided that Customer will not exercise this right more than once per year. Such responses are SparkPost's Confidential Information. If SparkPost is unable to provide all information necessary to demonstrate compliance with Article 28 Requirements through the written responses, then SparkPost will allow for and contribute to audits, including inspections, conducted by the Customer or another auditor representing the Customer. All information obtained from SparkPost during such audit or inspection is SparkPost's Confidential Information.

7. INTERNATIONAL TRANSFERS.
    1. **Processing Locations**. SparkPost may transfer and process Customer Data anywhere in the world where SparkPost, its Affiliates or its Sub-processors maintain data processing operations. SparkPost will at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.
    2. **Standard Contractual Clauses**. To the extent that SparkPost Processes any Personal Data under the Agreement that requires an onward transfer mechanism to lawfully transfer Personal Data from the EEA or the United Kingdom (the "**UK**") to another country or territory that has not been determined as providing an adequate level of protection for the rights and freedoms of Data Subjects by the European Commission (or, specifically with respect to the UK, as may be determined by the applicable UK regulatory body)(a "**Restricted Transfer**"), the parties agree as follows:
        1. **EEA Standard Contractual Clauses**. The parties agree to comply with the EEA Standard Contractual Clauses for any Restricted Transfer from the EEA (an "**EEA Restricted Transfer**"). When Customer is a Controller and SparkPost is a Processor as further described in Section 3.1, the Controller/Processor Standard Contractual clauses will apply to any such EEA Restricted Transfer. When Customer is a Processor and SparkPost is a Sub-processor as further described in Section 3.1, the Processor/Sub-processor Standard Contractual clauses will apply to any such EEA Restricted Transfer. SparkPost will be deemed the data importer and Customer will be deemed the data exporter under the EEA Standard Contractual Clauses. Each party's signing of this DPA, will be treated as signing of the applicable EEA Standard Contractual Clauses, which will be deemed incorporated into this DPA. Details required under Annex 1 and Annex 2 to the EEA Standard Contractual Clauses are available in Schedule 1 and Schedule 2 to this DPA. In the event of any conflict or inconsistency between this DPA and the EEA Standard Contractual Clauses, the EEA Standard Contractual Clauses shall prevail solely with respect to EEA Restricted Transfers. Where the EEA Standard Contractual Clauses require the parties to choose between optional clauses and to input information, the parties have done so as set out below:
            1. The Optional Clause 7 "Docking clause" shall not be adopted.
            2. For Clause 9 "Use of sub-processors", the parties elect the following option: "Option 2 General written authorisation: The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 calendar days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller

to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s)."

3. For Clause 11 (a) "Redress", the parties do not adopt the Option.
4. For Clause 17 "Governing law", the parties elect the following option: "Option 1. These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands."
5. For Clause 18 (b) "Choice of Forum and Jurisdiction": "The Parties agree that those shall be the courts of the Netherlands."

2. **UK Standard Contractual Clauses**. The parties agree to comply with the UK Standard Contractual Clauses for any Restricted Transfer from the UK (a "**UK Restricted Transfer**"). SparkPost will be deemed the data importer and Customer will be deemed the data exporter under the UK Standard Contractual Clauses. Each party's signing of this DPA, will be treated as signing of the UK Standard Contractual Clauses, which will be deemed incorporated into this DPA. Details required under Annex 1 and Annex 2 to the UK Standard Contractual Clauses are available in Schedule 1 and Schedule 2 to this DPA. In the event of any conflict or inconsistency between this DPA and the UK Standard Contractual Clauses, the UK Standard Contractual Clauses shall prevail solely with respect to UK Restricted Transfers.
3. **Cooperation**. If SparkPost is unable to comply with this requirement or if the relevant authorities or courts cease to recognize the EEA Standard Contractual Clauses or UK Standard Contractual Clauses, as applicable, as providing an adequate level of protection, SparkPost will inform Customer and reasonably cooperate with Customer to ensure that any Processing of Personal Data complies with Data Protection Laws and any transfer restrictions thereunder, including through achieving alternative certifications, as applicable and necessary.

3. **Alternative Transfer Mechanism**. The parties agree that the data export solution identified in Section 7.2 (Standard Contractual Clauses) will not apply if and to the extent SparkPost adopts, or maintains, an alternative data export solution for the lawful transfer of Personal Data (as recognized under Data Protection Laws) outside of the EEA and/or UK and which has been approved by Customer in writing prior to any transfer or other Processing of Personal Data ("**Alternative Transfer Mechanism**"), in which event, the Alternative Transfer Mechanism will apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

8. ADDITIONAL SECURITY.
    1. **Confidentiality of Processing**. SparkPost will ensure that any person who is authorized by SparkPost to process Personal Data (including its staff, agents and subcontractors) will be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).
    2. **Security Incident Response and Notification**. Upon becoming aware of a Security Incident, SparkPost will notify Customer without undue delay and will provide timely

information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

9. RETURN OR DELETION OF DATA.
    1. Upon termination or expiration of the Agreement, SparkPost will delete or return (at Customer's election) to Customer all Personal Data (including copies) in its possession or control, save that this requirement will not apply to the extent SparkPost is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data SparkPost will securely isolate and protect from any further processing, except to the extent required by applicable law.
10. COOPERATION.
    1. **Indemnification**. Both parties agree to defend and indemnify the other (including its directors, officers, employees and agents) from and against any third party claim (including from governmental authorities and Recipients) and related fees and expenses (including reasonable attorney's fees) arising out of its actual or alleged breach of this DPA.
    2. **Data Subject Requests**. The Service provides Customer with a number of controls that Customer may use to retrieve, correct, delete, or restrict Customer Data, which Customer may use to assist it in connection with its obligations under Data Protection Laws including, for example, its obligations relating to responding to Data Subject Requests. To the extent Customer is unable to independently access the relevant Customer Data within the Service, SparkPost will provide reasonable cooperation to assist Customer to timely respond to any Data Subject Request relating to the processing of Personal Data under the Agreement within any deadlines imposed by Data Protection Laws. In the event any such request is made directly to SparkPost, SparkPost shall notify Customer in writing of such request promptly upon receipt thereof.
    3. **Records of Processing**. Upon request from Customer, SparkPost will make available in a timely manner such information as is required by Customer to demonstrate SparkPost's compliance with its obligations under Data Protection Laws and under this DPA.
    4. **Government Requests**. If a law enforcement agency sends SparkPost a demand for Personal Data (for example, through a subpoena or court order), SparkPost will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, SparkPost may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then SparkPost will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless SparkPost is legally prohibited from doing so.
    5. **Data Protection Impact Assessments**. To the extent SparkPost is required under applicable Data Protection Laws, SparkPost will provide reasonably requested information regarding the Service to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law or pursuant to Articles 35 and 36 or GDPR, respectively.

***

SCHEDULE 1

ANNEX I TO THE EEA STANDARD CONTRACTUAL CLAUSES

Where applicable, this Schedule 1 will serve as Annex I to the EEA Standard Contractual Clauses.

ANNEX 1, PART A: LIST OF PARTIES

Data Exporter: Customer

Data Exporter Contact Details: The address listed in Customer's signature block above, or Customer's account owner email address, or to the email address(es) for which Customer elects to receive notices under the Agreement.

Data Exporter Role: The Data Exporter's role is outlined in Section 3 of the DPA.

Signature & Date: Data Exporter is deemed to have signed the EEA Standard Contractual Clauses incorporated herein as of the Effective Date of the DPA.

Data Importer: Message Systems, Inc. (dba SparkPost)

Data Importer Contact Details: SparkPost Data Protection Officer – privacy@sparkpost.com

Data Importer Role: The Data Importer's role is outlined in Section 3 of the DPA.

Signature & Date: Data Importer is deemed to have signed the EEA Standard Contractual Clauses incorporated herein as of the Effective Date of the DPA.

ANNEX 1, PART B: DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred is described in Section 3.4 of the DPA.

Categories of personal data transferred is described in Section 3.4 of the DPA.

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:

- None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

- Data is transferred on a continuous basis for the duration of the Agreement.

Nature of the processing is described in Section 3.4 of the DPA.

Purpose(s) of the data transfer and further processing is described in Section 3.4 of the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

- For the duration of the Agreement or longer as required by applicable law and as permitted by the Agreement.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing:

- For transfers to sub-processors, the subject matter and nature of the processing is outlined at https://www.sparkpost.com/policies/subprocessors/ and the duration is for the duration of the Agreement.

ANNEX 1, PART C: COMPETENT SUPERVISORY AUTHORITY

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) will be the competent supervisory authority.

***

SCHEDULE 2

ANNEX II TO THE EEA STANDARD CONTRACTUAL CLAUSES

Where applicable, this Schedule 2 will serve as Annex II to the Standard Contractual Clauses. The following provides more information regarding SparkPost's technical and organizational security measures set forth below.

More information about SparkPost's technical and organizational security measures to protect Customer Data, a summary of which is available at: https://www.sparkpost.com/policies/security/ ("Security Policy").

Technical and Organizational Security Measures:

Measures of pseudonymization and encryption of personal data: SparkPost maintains Customer Data in an encrypted format at rest and in transit using SSL, HTTPS, and opportunistic TLS as applicable.

Measures for ensuring ongoing confidentiality, integrity, and availability and resilience of processing systems and services: SparkPost agrees to confidentiality obligations in its agreements with its customers. SparkPost also enters into agreements that contain substantively similar confidentiality provisions with SparkPost's employees, contractors, vendors, and sub-processors. SparkPost maintains high availability and resiliency of the systems and services through multiple fault-independent data center availability zones. Additionally, SparkPost has implemented and maintains a Business Continuity and Disaster Recovery Plan to ensure Customer Data is preserved and the Services can continue to be provided.

Measures for ensuring the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident: Customer Data is hosted by Amazon Web Services ("AWS"), which provides redundancy across multiple availability zones. As stated above, SparkPost also has implemented and maintains a Business Continuity and Disaster Recovery Plan.

Processes for regular testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of processing: SparkPost maintains a written and comprehensive information security program, which includes appropriate physical, technical, and administrative controls to protect the security, integrity, confidentiality, and availability of Customer Data including, without limitation, protecting Customer Data against any unauthorized or unlawful acquisition, access, use, disclosure, or destruction. This security program was designed taking into account the type of services SparkPost provides and the size and complexity of SparkPost's business. In addition to our in-house security team who consistently monitor our security internally, SparkPost uses a third party to conduct internal and external vulnerability and penetration testing to validate the perimeter and internal defensive posture on a regular cadence.

Measures for user identification and authorization: SparkPost employees are required to use unique user access credentials and passwords for authorization. SparkPost utilizes the principles of least privilege access when provisioning system access, which takes into account each employee's job function, role and responsibilities when determining the appropriate level and duration of access.

Access requires approval prior to provisioning and access is promptly removed upon role change or termination.

Measures for the protection of data during transmission: Customer Data is encrypted when in transit between Customer and SparkPost Services using HTTPS. Customer Data is encrypted when in transit between SparkPost and Recipient using opportunistic TLS.

Measures for the protection of data during storage: Customer Data is stored encrypted using the Advanced Encryption Standard.

Measures for ensuring physical security of locations at which personal data are processed: SparkPost headquarters and office spaces have (i) physical security monitoring and surveillance; (ii) entry controls to limit physical access; and (iii) visitor logs. All contractors and visitors are required to log their entry and exit into the offices. The Services operate on AWS and are protected by the physical, technical, organizational, and administrative controls of Amazon. Detailed information about AWS security is available at https://aws.amazon.com/security/, https://aws.amazon.com/security/sharing-the-security-responsibility/, and https://aws.amazon.com/compliance/iso-27001-faqs/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/.

Measures for ensuring events logging: SparkPost's production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

Measures for ensuring systems configuration, including default configuration: SparkPost evaluates changes to its platform, applications, and production infrastructure in a manner that minimizes risk and such changes are implemented only in accordance with the Security Policy. SparkPost performs numerous security-related activities for the Services across different phases of the product creation lifecycle from creating requirements documentation and product design all the way through the go-live stage. These activities include the performance of (i) internal security reviews before new Services are deployed; (ii) annual penetration testing by independent third parties; and (iii) threat analysis for new Services to detect any potential security threats and vulnerabilities. SparkPost adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. Monitoring is in place to notify the security team of changes made to critical infrastructure and services that do not adhere to the change management processes.

Measures for internal IT and IT security governance and management: SparkPost maintains a risk-based assessment security program, which includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. SparkPost's security program was designed taking into account the nature of the Services and the size and complexity of SparkPost's business. SparkPost has a dedicated security team that manages SparkPost's information security program and facilitates and supports independent audits and assessments performed by third parties. SparkPost's security framework is based on the SOC2 Type II attestation and includes the following trust services criteria:

Security, Availability, Confidentiality, and Privacy. Security is managed at the highest levels of the company, with the VP of Compliance and IT Security meeting with executive management regularly to discuss issues and coordinate company-wide security and IT initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all relevant SparkPost employees for their reference.

Measures for certifications/assurance of processes and products: SparkPost conducts various third-party audits to attest to various frameworks including SOC 2 Type II and regular application vulnerability and penetration testing.

Measures for ensuring data minimization: SparkPost does not store the message body of an Email after it has either been delivered to the Recipient or has bounced or otherwise been rejected by the mailbox provider, which typically occurs within seconds. In the event of a rejection or bounce, SparkPost will retain the message body for a limited period of time to allow for the Email transmission to be retried. If the transmission is still unsuccessful, the message body is permanently deleted. SparkPost only stores Recipient Personal Data in raw form for a limited amount of time after the transmission of an Email to a Recipient. After the initial retention period, the Personal Data is pseudonymized through a one-way hash and is only stored in its pseudonymized form. For more information about this process please see our Data FAQs available at: https://www.sparkpost.com/policies/data-faq/. Additionally, SparkPost has built in self-service functionality to the Services that allow Customers to delete certain Customer Data, like Recipient email addresses and associated message events, on demand, which documentation for such functionality is available at: https://developers.sparkpost.com/api/data-privacy/.

Measures for ensuring accountability: SparkPost has adopted measures for ensuring accountability including conducting regular third-party audits to ensure compliance with our privacy and security standards. SparkPost also implements data protection policies in accordance with applicable law and publishes an overview of the Security Policy (linked above). SparkPost has appointed a Data Protection Officer and maintains documentation of its processing activities, including recording and reporting Security Incidents involving Personal Data where applicable.

Measures for allowing data portability and ensuring erasure: Customers have direct relationships with their Recipients and are responsible for responding to requests from their end users who wish to exercise their rights under Data Protection Laws. SparkPost has built in self-service functionality to the Services that allow Customers to delete certain Customer Data, like Recipient email addresses and associated message events on demand, which documentation for such functionality is available at: https://developers.sparkpost.com/api/data-privacy/. Additionally, SparkPost has built in self-service functionality to suppress future Emails to Recipients (i.e., unsubscribe), which documentation for such functionality is available at https://developers.sparkpost.com/api/suppression-list/. To the extent Customer is unable to independently access the relevant Customer Data within the Service, SparkPost will provide reasonable cooperation to assist Customer to timely respond to any Data Subject Request relating to the processing of Personal Data under the Agreement within any deadlines imposed by Data Protection Laws. In the event any such request is made directly to SparkPost, SparkPost will advise

the Data Subject to submit their request to Customer, and Customer will be responsible for responding to any such request.

For transfers to [sub]-processors, also describe the specific technical and organisational measures to be taken by the [sub]-processor to be able to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the data exporter: When SparkPost engages a sub-processor under this DPA, SparkPost and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein.

V2.0 November 2, 2021