October 27, 2020

Data Processing Agreement

This Data Processing Agreement (this "**DPA**") forms part of the Mailgun Terms of Service (the "**Principal Agreement**") by and between Mailgun Technologies, Inc. on its own behalf and on behalf of its Affiliates ("**Mailgun**") and Evidence Based Education (the "**Customer**") and is subject to the Principal Agreement.

1. Definitions. For the purposes of this DPA, capitalized terms shall have the following meanings. Capitalized terms not otherwise defined shall have the meaning given to them in the Principal Agreement.

(a) **"Affiliates"** means any entity that is owned or that owns Mailgun Technologies, Inc. or that is under common control with one of Mailgun's entities, including but not limited to Mailgun Technologies SAS and Mailjet SAS.

(b) **"Customer's Personal Data**" means any personal data that is processed by Mailgun on behalf of the Customer to perform the Services under the Principal Agreement.

(c) **"EU Data Protection Laws"** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including (with effect from May 25, 2018) by the GDPR and laws implementing, replacing or supplementing the GDPR.

(d) "**GDPR**" means EU General Data Protection Regulation 2016/679.

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

(f) **"Mailgun Infrastructure"** means (i) Mailgun physical facilities; (ii) hosted cloud infrastructure; (iii) Mailgun's corporate network and the non-public internal network, software, and hardware necessary to provide the Services and which is controlled by Mailgun; in each case to the extent used to provide the Services.

(g) "**Restricted Transfer**" means a transfer of the Customer's Personal Data from Mailgun to a sub-processor where such transfer would be prohibited by EU Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of EU Data Protection Laws) in the absence of appropriate safeguards required for such transfers under EU Data Protection Laws.

(h) "**Services**" means the services provided to the Customer by Mailgun pursuant to the Principal Agreement.

(i) "**Standard Contractual Clauses**" means the latest version of the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (the current version as at the date of this DPA is annexed to European Commission Decision 2010/87/EU).

(j) The terms "**consent**", "**controller**", "**data subject**", "**Member State**", "**personal data**", "**personal data breach**", "**processor**", "**sub processor",** "**processing**", "**supervisory authority**" and "**third party**" shall have the meanings ascribed to them in article 4 of the GDPR.

2. Compliance with EU Data Protection Laws

(a) Mailgun and the Customer shall each comply with the provisions and obligations imposed on them by the EU Data Protection Laws and shall procure that their employees, agents and contractors observe the provisions of the EU Data Protection Laws.

3. Details and Scope of the Processing

(a) The Processing of the Customer's Personal Data within the scope of the Agreement shall be carried out in accordance with the following stipulations and as required under Article 28(3) of the GDPR. The parties may amend this information from time to time, as the parties may reasonably consider necessary to meet those requirements.

(i) **Subject matter and duration of the processing of Personal Data:** The subject matter and duration of the processing of the Personal Data are set out in the Principal Agreement.

(ii) **The nature and purpose of the processing of Personal Data:** Under the Principal Agreement, Mailgun provides certain email and sms services to the Customer which involves the processing of personal data. Such processing activities include (a) providing the Services; (b) the detection, prevention and resolution of security and technical issues; and (c) responding to Customer's support requests.

(iii) **The types of Personal Data to be processed:** The personal data submitted, the extent of which is determined and controlled by the Controller in its sole discretion, includes name, email, telephone numbers IP address and other personal data included in the contact lists and message content.

(iv) **The categories of data subject to whom the Personal Data relates:** Senders and recipients of email and sms messages.

(b) Mailgun shall only process the Customer's Personal Data (i) for the purposes of fulfilling its obligations under the Principal Agreement and (i) in accordance with

the documented instructions described in this DPA or as otherwise instructed by the Customer from time to time. Such Customer's instructions shall be documented in the applicable order, services description, support ticket, other written communication or as directed by Customer using the Services (such as through an API or control panel).

(c) Where Mailgun reasonably believes that a Customer instruction is contrary to the provisions of the Principal Agreement or this DPA, or that it infringes the GDPR or other applicable data protection provisions, it shall inform the Customer without delay. In both cases, Mailgun shall be authorized to defer the performance of the relevant instruction until it has been amended by Customer or is mutually agreed by both Customer and Mailgun.

(d) Customer is solely responsible for its utilization and management of Personal Data submitted or transmitted by the Services, including: (i) verifying recipient's addresses and that they are correctly entered into the Services (ii) reasonably notifying any recipient of the insecure nature of email as a means of transmitting Personal Data (as applicable), (iii) reasonably limiting the amount or type of information disclosed through the Services (iv) encrypting any Personal Data transmitted through the Services where appropriate or required by applicable law (such as through the use of encrypted attachments, PGP toolsets, or S/MIME). When the Customer decides not to configure mandatory encryption, the Customer acknowledges that the Services may include the transmission of unencrypted email in plain text over the public internet and open networks. Information uploaded to the Services, including message content, is stored in an encrypted format when processed by the Mailgun Infrastructure.

4. Controller and Processor

(a) For the purposes of this DPA, the Customer is the controller of the Customer's Personal Data and Mailgun is the processor of such data, except when the Customer acts as a processor of the Customer's Personal Data, in which case Mailgun is a sub-processor.

(b) Mailgun shall at all times have in place an officer who is responsible for assisting the Customer (i) in responding to inquiries concerning the Data Processing received from Data Subjects; and, (ii) in completing all legal information and disclosure requirements which apply and are associated with the Data Processing. The Data Protection Officer may be contacted directly at privacy@mailgun.com.

(c) The Customer warrants that:

(i) The processing of the Customer's Personal Data is based on legal grounds for processing, as may be required by EU Data Protection Laws and that it has made and shall maintain throughout the term of the Principal Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by EU Data Protection Laws with respect

to Mailgun's processing of the Customer's Personal Data under this DPA and the Principal Agreement;

(ii) it is entitled to and has all necessary rights, permissions and consents to transfer the Customer's Personal Data to Mailgun and otherwise permit Mailgun to process the Customer's Personal Data on its behalf, so that Mailgun may lawfully use, process and transfer the Customer's Personal Data in order to carry out the Services and perform Mailgun's other rights and obligations under this DPA and the Principal Agreement;

(iii) it will inform its Data Subjects about its use of Processors in Processing their Personal Data, to the extent required under applicable EU Data Protection Laws; and,

(iv) it will respond in a reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data, and to give appropriate instructions to the Processor in a timely manner.

5. Confidentiality

(a) Mailgun shall ensure that each of its, and sub-processors', personnel that is authorized to process the Customer's Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality and are trained with the relevant security and Data Protection requirements.

6. Technical and Organizational Measures

(a) Mailgun shall, in relation to the Customer's Personal Data, (a) take and document, as appropriate, reasonable and appropriate measures required pursuant to Article 32 of the GDPR in relation to the security of the Mailgun Infrastructure and the platforms used to provide the Services as described in the Principal Agreement, and (b) on reasonable request at the Customer's cost, assist the Customer in ensuring compliance with the Customer's obligations pursuant to Article 32 of the GDPR.

(b) Mailgun’s internal operating procedures shall comply with the specific requirements of an effective Data Protection management.

7. Data Subject Requests

(a) Mailgun provides specific tools in order to assist customers in replying to requests received from data subjects. These include our APIs and interfaces to search event data, suppressions, and retrieve message content. When Mailgun receives a complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to EU Data Protection Laws) related to the Customer's Personal Data directly from data subjects Mailgun will notify the

Customer within 14 days from the receipt of the complaint, inquiry or request. Taking into account the nature of the processing, Mailgun shall assist the Customer at the Customer's cost, by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfillment of the Customer's obligation to respond to requests for exercising such data subjects' rights.

8. Personal Data Breaches

(a) Mailgun shall notify the Customer without undue delay once Mailgun becomes aware of a personal data breach affecting the Customer's Personal Data. Mailgun shall, taking into account the nature of the processing and the information available to Mailgun, use commercially reasonable efforts to provide the Customer with sufficient information to allow the Customer at the Customer's cost, to meet any obligations to report or inform regulatory authorities, data subjects and other entities of such personal data breach to the extent required under EU Data Protection Laws.

9. Data Protection Impact Assessments

(a) Mailgun shall, taking into account the nature of the processing and the information available, provide reasonable assistance to the Customer at the Customer's cost, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for the Customer to fulfill its obligations under EU Data Protection Laws.

10. Audits

(a) Mailgun shall make available to the Customer on reasonable request, information that is reasonably necessary to demonstrate the Customer's compliance with this DPA.

(b) Customer, or a mandated third party auditor, may upon written reasonable request conduct an inspection in relation to the Processing of the Customer’s Personal Data by Mailgun and to the extent necessary according to Data Protections Laws and without interrupting Mailgun’s business operations and ensuring confidentiality. The Customer shall be responsible for any costs and expenses of Processor arising from the provision of such audit rights.

11. Return or Destruction of the Customer's Personal Data

(a) The Customer may, by written notice to Mailgun, request the return and/or certificate of deletion of all copies of the Customer's Personal Data in the control or possession of Mailgun and sub-processors. Mailgun shall provide a copy of the Controller's Data in a form that can be read and processed further.

(b) Within ninety (90) days following termination of the account, the Processor shall delete and/or return all Personal Data processed pursuant to this DPA. This provision shall not affect potential statutory duties of the Parties to preserve records for retention periods set by law, statute or contract. Mailgun may retain electronic copies of files containing Customer's Personal Data created pursuant to automatic archiving or back-up procedures which cannot reasonably be deleted. In these cases, Mailgun shall ensure that the Customer's Personal Data is not further actively processed.

(c) Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by the Customer.

12. Data Transfers

(a) Following execution of this DPA, Mailgun shall, if requested to do so by the Customer and if required by EU Data Protection Laws, enter into the Standard Contractual Clauses as data importer with the Customer acting as data exporter. If Mailgun's arrangement with a sub-processor involves a Restricted Transfer, Mailgun shall ensure that the onward transfer provisions of the Standard Contractual Clauses are incorporated into the Principal Agreement, or otherwise entered into, between Mailgun and the sub-processor. The Customer agrees to exercise its audit right in the Standard Contractual Clauses by instructing Mailgun to conduct the audit set out in Paragraph 10.

(b) Controller acknowledges and agrees that, in connection with the performance of the Services under the Agreement, Processor may transfer Personal Data within its company group. These transfers are necessary to globally provide the Services, and are justified for internal administration purposes.

(c) For transfers of Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of Data Protection within the meaning of Data Protection Laws of the foregoing territories, to the extent such transfers are subject to Data Protection Laws and Regulations and in order to implement appropriate safeguards, the following safeguards are taken: (i) Standard Contractual Clauses as per European Commission's Decision 2010/87/EU and, (2) additional safeguards with respect to security measures including data encryption and data minimization principles.

13. Sub-processing

(a) The Customer hereby authorizes Mailgun to appoint sub-processors in accordance with this Paragraph 12 and Annex 2, subject to any restrictions in the Principal Agreement. Mailgun will ensure that sub-processors are bound by written agreements that require them to provide at least the level of data protection required of Mailgun by this DPA. Mailgun may continue to use those sub-processors already engaged as at the date of this DPA.

(b) Mailgun shall give the Customer prior written notice of the appointment of any new sub-processor. If, within ten (10) business days of receipt of that notice, the Customer notifies Mailgun in writing of any objections on reasonable grounds to the proposed appointment, Mailgun shall not appoint that proposed sub-processor until reasonable steps have been taken to address the objections raised by the Customer and the Customer has been provided with a reasonable written explanation of the steps taken. If Mailgun and the Customer are not able to resolve the appointment of a sub-processor within a reasonable period, either party shall have the right to terminate the Principal Agreement for cause.

(c) In addition, in the event of authorized sub-contracting outside the European Union, the Customer mandates Mailgun to enter into EU Model Clauses in its name and on its behalf for the specific purposes of the providing the services under the Principal Agreement.

(d) This paragraph does not apply to the following ancillary services, namely telecommunication services, postal or transport services, maintenance and user support tools. Mailgun shall, however, be obligated to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the Data protection and Data security of the Customer's Data even for these outsourced ancillary services.

(e) Mailgun shall be responsible for the acts and omissions of any sub-processors as it is to the Customer for its own acts and omissions in relation to the matters provided in this DPA.

14. Governing law and jurisdiction

(a) The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

(b) This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

15. Order of precedence

(a) With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

16. Changes in Data Protection Laws, etc.

a. Mailgun may modify or supplement this DPA, with reasonable notice to the Customer:

i. If required to do so by a supervisory authority or other government or regulatory entity;

ii. If necessary to comply with applicable law;

iii. To implement new or updated Standard Contractual Clauses approved by the European Commission; or

iv. To adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 GDPR.

17. Severance

(a) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

18. Termination

(a) This DPA and the Standard Contractual Clauses will terminate contemporaneously and automatically with the termination of the Principal Agreement.

(b) Mailgun may terminate this DPA and the Standard Contractual Clauses if Mailgun offers alternative mechanisms to Customer that comply with the obligations of the European Union privacy laws for the transfer of Personal Data outside the EEA.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

Mailgun Technologies, Inc.

Signature: DocuSigned by: Josh Odom DA0F8F5ED7BE40A...

Name: Josh Odom

Title: CTO

Date Signed 23/10/2020

The Customer

Signature: DocuSigned by: Jack Deverson D615F6ECDED64C4...

Name: Jack Deverson

Title: Managing Director

Date Signed: 6/17/2021

ANNEX 1

INFORMATION SECURITY - TECHNICAL AND ORGANIZATIONAL MEASURES

Where personal data is processed or used automatically, Mailgun's internal organization ensures that it meets specific requirements of data protection by utilizing security best practices. In particular, Mailgun implements the following measures to protect personal data or other sensitive data categories.

Physical Access Control

To prevent unauthorized persons from gaining access to data processing systems with which personal data is processed or used:

- Mailgun leverages industry-leading data center and cloud infrastructure providers. Access to all data centers is strictly controlled. All data centers are equipped with 24x7x365 surveillance and biometric access control systems. Additionally, all providers are SOC Type II and ISO 27001 certified.
- Data centers are equipped with at least N+1 redundancy for power, networking, and cooling infrastructure.
- Within a region, data processing occurs across at least three distinct availability zones. Services are designed to withstand the failure of an availability zone without customer disruption.

System Access Control

To prevent data processing systems from being used without authorization:

- Administrative access to Mailgun systems and services follows the principle of least privilege. Access to systems is based on job role and responsibilities. Mailgun utilizes unique usernames/identifiers that are not permitted to be shared or re-assigned to another person.
- VPN and multi-factor authentication is used for access to internal support tools and product infrastructure.
- Network access control lists (ACLs) and security groups are used to limit ingress and egress traffic from production infrastructure.
- Intrusion detection systems (IDS) are used to detect potential unauthorized access.
- Network protections have been deployed to mitigate the impact of distributed denial of service (DDoS) attacks.
- Onboarding and offboarding processes are documented and followed consistently to ensure access is properly managed to internal and externally hosted tools and systems. Where possible, third-party services leverage single sign-on (SSO) functionality which allows for centralized management and enforces multi-factor authentication.

Data Access Control

To ensure authorized users entitled to use data processing systems have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage:

- Mailgun utilizes a password management system that enforces minimum password length, complexity, expiration time, and minimum last used.
- Employee workstations automatically lock after a prolonged period of inactivity. Systems log out users after a prolonged period of inactivity.
- Logs are centrally stored and indexed. Critical logs, such as security logs, are retained for at least one year.
- The Mailgun patch management process ensures that systems are patched at least once every month. Monitoring, alerting, and routine vulnerability scanning occurs to ensure that all product infrastructure is patched consistently.
- Industry-standard antivirus software is utilized to ensure internal assets that access personal data are protected against known viruses. Antivirus software is updated regularly.
- Mailgun utilizes firewalls to segregate unwanted traffic from entering the network. A DMZ is utilized using firewalls to further protect internal systems protecting sensitive data.

Data Transmission Control

To ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport:

- Customer data is stored encrypted-at-rest through the use of AES-256 encryption on block devices.
- Customer backups are encrypted-in-transit and at rest using strong encryption.
- Mailgun supports TLS 1.0, 1.1, and 1.2 to encrypt network traffic between the client application and Mailgun infrastructure. Customers can control and manage encryption settings for messages processed by Mailgun and sent to receiving mailbox providers to achieve compliance needs beyond the scope of Mailgun's external certifications.
- Mailgun is alerted to encryption issues through periodic risk assessments and third-party penetration tests. Mailgun performs third-party penetration tests on an annual basis, or as needed due to changes in the business.
- Mailgun operates a bug bounty program, encouraging the responsible disclosure of vulnerabilities from community researchers.

Input Control

To ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed:

- Systems are monitored for security events to ensure quick resolution.

- Logs are centrally stored and indexed. Critical logs, such as security logs, are retained for at least one year. Logs can be traced back to individual unique usernames with timestamps to investigate nonconformities or security events.

Availability Control

To ensure personal data is protected from accidental destruction or loss:

- Account data is backed up at least daily. Incremental/point-in-time recovery is available for all primary databases. Backups are encrypted-in-transit and at rest using strong encryption.
- Mailgun patch management process ensures that systems are patched at least once every month. Monitoring, alerting, and routine vulnerability scanning occurs to ensure that all product infrastructure is patched consistently.
- When necessary, Mailgun patches infrastructure in an expedited manner in response to the disclosure of critical vulnerabilities to ensure system uptime is preserved.
- Customer environments are logically separated at all times. Customers are not able to access accounts other than those given authorization credentials for.

ANNEX 2

AUTHORIZED SUB-PROCESSORS AS OF THE DPA EFFECTIVE DATE

Infrastructure Sub-Processors				
Company	**Server Location**	**Description of Activities**	**Appropriate Safeguards for transfers**	**Applicable Services**
Google Platform	Germany & Belgium (EU customers) USA (US customers)	Datacenter	EU law EU Model Clauses Data encryption	All services
Rackspace (AWS)	USA (US customers) Germany (EU customers)	Datacenter	EU law EU Model Clauses Data encryption	All services
Support Sub-Processors				
Company	**Location**	**Description of Activities**	**Appropriate Safeguards for transfers**	**Applicable Services**
Proxiad Bulgaria	Bulgaria	Ticket support functions TAM functions	EU law Data minimization	All services
Sitel India	India	Ticket support functions	EU Model Clauses Data encryption Data minimization	All services
Group Company Sub-Processors				
Company	**Headquarters**	**Description of Activities**	**Appropriate Safeguards for transfers**	**Applicable Services**
Mailgun Technologies	USA	Group company	EU Model Clauses	All services
Mailjet	France	Group company	EU Model Clauses EU law	All services

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

The Customer entity that is a party to the DPA to which these Standard Contractual Clauses are attached.

AND

Mailgun Technologies, Inc.
112 E Pecan St #1135
San Antonio, TX 78205
legal@mailgun.com

(the **data importer** or **data sub processor (as applicable)**)

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.

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[1];

(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

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 sub processor'* means any processor engaged by the data importer or by any other sub processor of the data importer who agrees to receive from the data importer or from any other sub processor 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 organizational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 sub processor 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 sub processor 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 organizational 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, unauthorized 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 sub processor 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 sub processing 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 sub processing, the processing activity is carried out in accordance with Clause 11 by a sub processor 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[2]

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 organizational 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 unauthorized access, and

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

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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 sub processing, 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 sub processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub processor 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 sub processor 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 sub processor 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 sub processor 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 sub processor 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 sub processor agrees that the data subject may issue a claim against the data sub processor 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 sub processor 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 sub processor, 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 sub processor preventing the conduct of an audit of the data importer, or any sub processor, 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

Sub processing

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 sub processor which imposes the same obligations on the sub processor as are imposed on the data importer under the Clauses. Where the sub processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub processor 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 sub processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub processing 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 sub processing 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 sub processor 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 sub processor 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 Mailgun Technologies, Inc.:

Name: Josh Odom
Position: CTO
112 E Pecan St #1135
San Antonio, TX 78205

Signature: DocuSigned by: Josh Odom DA0F8F5ED7BE40A...

On behalf of the Customer

Name (written out in full): Jack Deverson

Position: Managing Director

Address: 1 Grange Crescent, Sunderland SR2 7BN

Signature: DocuSigned by: Jack Deverson D615F6ECDED64C4...

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

DATA EXPORTER

The data exporter is the non-Mailgun entity that transfers Personal Data outside the EEA and uses Mailgun services as a direct Customer of Mailgun or as an end user through Mailgun's Customer.

DATA IMPORTER

The data importer is Mailgun Technologies, Inc., a provider of Mailgun™ services.

DATA SUBJECTS

The personal data transferred may concern individuals about whom personal data is transmitted or stored by data exporter via the Mailgun hosted system and/or services.

CATEGORIES OF DATA

The personal data transferred includes name, email, IP address and personal data included in message content.

PROCESSING OPERATIONS

Under the Agreement, Mailgun provides certain email services to the data exporter or data importer, as applicable. Mailgun may therefore process personal data. Such processing activities include (a) providing the Services; (b) the detection, prevention and resolution of security and technical issues; and (c) responding to Customer's support requests.

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 organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer shall implement security measures equivalent to those required under the Agreement, the DPA and any ancillary documents entered into pursuant to the Agreement.

For the purpose of securing the personal data processed, Mailgun uses industry best practices as described in Annex 2 of this agreement.