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

(b) **"EU Data Protection Laws"** means the GDPR, as transposed into domestic legislation of each Member State (and the United Kingdom) and as amended, replaced or superseded from time to time, and laws implementing, replacing or supplementing the GDPR.

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

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

(e) **"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.

(f) "**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.

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

(h) "**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 the GDPR (the current version as at the date of this DPA is as annexed to European Commission Decision 2021/914 (EU) of June 4, 2021).

(i) "Subsidiaries" means the following entities owned or controlled by Mailgun Technologies, Inc.: Mailjet SAS and its subsidiaries.

(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 subjects 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, 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 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 the 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 2021/914/EU of June 4, 2021 and, (2) additional safeguards with respect to security measures including data encryption, data aggregation, separation of access controls and data minimization principles.

13. Sub-processing

(a) The Customer hereby authorizes Mailgun to appoint sub-processors in accordance with this Paragraph 13 and Annex 1, 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 Standard Contractual Clauses in its name and on its behalf for the specific purposes of 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. 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.

17. Termination

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

(b) Any amendment or variation to this DPA shall not be binding on the Parties unless set out in writing and signed by authorised representatives of each of the Parties.

* * *

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

Mailgun Technologies, Inc.	**The Customer**
Signature: DocuSigned by: Josh Odom DA0F8F5ED7BE40A...	Signature:
Name: Josh Odom	Name: Iulia Stanciu
Title: CTO	Title:
1/11/2022	Date Signed:

ANNEX 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

For the purposes of these SCCs, 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, and the Standard Contractual Clauses - Processor to Processor (Module 3) will be applicable in this latter event.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of data to a third country.

(b) The Parties:

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

the "data importer" (the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses)

(ii) the Customer entity that is a party to the DPA to which these Standard Contractual Clauses are attached (hereinafter "data exporter")

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Paragraph 3 of the DPA.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Paragraph 3 of the underlying DPA.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by signing an amendment to these Clauses.

(b) Once it has signed an amendment to these Clauses, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in the DPA.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Paragraph 3 of the underlying DPA, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including any Annexes as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex 2 and personal data, the data exporter may redact part of the text of the Annexes to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in the underlying DPA. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in the Annexes.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) business days in advance, thereby giving the data exporter 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 data exporter

with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by

which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer: CNIL, the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*), shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with

these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[1];

[1] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such

notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with

these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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 France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX 2

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 firewall devices 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.

Certification/assurance of processes and products

To ensure internal IT and IT security governance and management as well as assurance of processes and products

- ISO 27001 certification
- ISO 27701 certification
- SOC 2 Type 2 report

ANNEX 3

AUTHORIZED SUB-PROCESSORS AS OF THE DPA EFFECTIVE DATE

Infrastructure Sub-Processors			
Company	**Server Location**	**Description of Activities**	**Appropriate Safeguards for transfers**
Google Cloud Platform 70 Sir John Rogerson's Quay, Dublin 2, Ireland	Germany & Belgium (EU customers) USA (US customers)	Datacenters	SCCs Data encryption
Rackspace (AWS) One Fanatical Place San Antonio, TX 78218 USA	USA (US customers) Germany (EU customers)	Datacenters	SCCs Data encryption
Support Sub-Processors			
Company	**Location**	**Description of Activities**	**Appropriate Safeguards for transfers**
Proxiad Bulgaria Tintyava 13b St., Fl. 4 Sofia 1113 - Bulgaria	Bulgaria	Ticket support functions TAM functions	EU law Data minimization
Sitel India Chandivali – Farm Road, Andheri East Mumbai 400072 India	India	Ticket support functions *(provide first response through ticketing system; no access to customer personal data*)	SCCs Data encryption Data minimization
Group Company Sub-Processors			
Company	**Headquarters**	**Description of Activities**	**Appropriate Safeguards for transfers**
Mailgun Technologies 112 E. Pecan Street #1135, San Antonio, Texas, 78205 USA	USA	Group company *(Administrative, billing, support and maintenance services)*	SCCs Data encryption Data minimization
Mailjet 4, rue Jules Lefebvre 75009 Paris, France	France	Group company	SCCs Data encryption Data aggregation
Sinch AB Lindhagensgatan 74 Stockholm, 112 18 Sweden	Sweden	Group company	SCCs Data encryption Data aggregation