DATA PROTECTION ADDENDUM

Effective: October 21, 2020

This Data Protection Addendum ("*Addendum*") supplements the agreement between Customer and Twilio into which it is incorporated by reference ("*Agreement*").

I. Introduction

1. **Definitions.**

. *"Applicable Data Protection Law*" refers to all laws and regulations applicable to Twilio's processing of personal data under the Agreement including, without limitation, the General Data Protection Regulation (EU 2016/679) ("*GDPR*").

. *"controller"*, "*processor*", "*data subject*", "*personal data,*" and "*processing*" (and "*process*") have the meanings given in accordance with Applicable Data Protection Law.

. *"Customer Account Data"* means personal data that relates to Customer's relationship with Twilio, including the names and/or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Customer Account Data also includes any data Twilio may need to collect for the purpose of identity verification, or as part of its legal obligation to retain subscriber records.

. *"Customer Content"* means (a) personal data exchanged by means of use of the Services, such as text, message bodies, voice and video media, images, email bodies, email recipients, and

sound, and (b) data stored on Customer's behalf such as communication logs within the Services or marketing campaign data Customer has uploaded to the SendGrid Services.

. *"Customer Data"* has the meaning given in the Agreement. Customer Data includes Customer Account Data, Customer Usage Data, Customer Content and Sensitive Data, as defined in this Addendum.

. *"Customer Usage Data"* means data processed by Twilio for the purposes of transmitting or exchanging Customer Content, including data used to identify the source and destination of a communication, such as (a) individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Services, and the date, time, duration and the type of communication and (b) activity logs used to identify the source of Service requests, optimize and maintain performance of the Services, and investigate and prevent system abuse.

. *"Privacy Policy"* means the then-current privacy policy for the Services available at https://www.twilio.com/legal/privacy (https://www.twilio.com/legal/privacy).

. *"Security Controls"* means the terms set forth in the Agreement outlining Twilio's technical and organisational measures to protect Customer Data, or, if the Agreement has no such terms, then the Twilio Security Overview available at https://www.twilio.com/legal/security-overview.

. *"Security Incident"* means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

. *"SendGrid Services"* means the services enabling companies to develop, transmit, analyze, and manage email communications and other related digital communications and tools through the website at https://www.sendgrid.com (http://www.sendgrid.com), including all programs, features, functions and report formats, and subsequent updates or upgrades of any of the foregoing made generally available by Twilio. The SendGrid Services excludes any Twilio Services.

. *"Sensitive Data"* has the meaning given in the Twilio Acceptable Use Policy available at https://www.twilio.com/legal/aup (https://www.twilio.com/legal/aup).

. *"Services"* means, collectively, the Twilio Services and SendGrid Services.

. *"Twilio Services"* means the products and services that are ordered by Customer under an Order Form or by using a Twilio account, or provided by Twilio to Customer on a trial basis or otherwise free of charge. Twilio Services generally consist of: (a) platform services, namely access to the Twilio application programming interface (referred to herein as Twilio APIs) and, where applicable, and (b) connectivity services, that link the Twilio Services to the telecommunication providers' networks via the Internet. The Twilio Services exclude any SendGrid Services.

Any capitalized term used but not defined in this Addendum has the meaning provided to it in the Agreement.

II. Controller and Processor

2. Relationship of the Parties.

2.1 Twilio as a Processor. The parties acknowledge and agree that with regard to the processing of Customer Content, Customer may act either as a controller or processor and Twilio is a processor.

2.2 Twilio as a Controller of Customer Account Data. The parties acknowledge that, with regard to the processing of Customer Account Data, Customer is a controller and Twilio is an independent controller, not a joint controller with Customer.

2.3 Twilio as a Controller of Customer Usage Data. The parties acknowledge that, with regard to the processing of Customer Usage Data, Customer may act either as a controller or processor and Twilio is an independent controller, not a joint controller with Customer.

3. Purpose Limitation. Twilio will process personal data in order to provide the Services in accordance with the Agreement. Section 2.1 of Schedule 1 (Details of Processing) further specifies the duration of the processing, the nature and purpose of the processing, and the types of personal data and categories of data subjects. Twilio will process Customer Content in accordance with Customer's instructions as outlined in Section 5 (Customer Instructions). Twilio will process Customer Account Data and Customer Usage Data in accordance with Applicable Data Protection Law and consistent with the Privacy Policy, the Agreement, and this Addendum.

4. Compliance. Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the Services and its own processing of personal data and (b) it has, and will continue to have, the right to transfer, or provide access to, the personal data to Twilio for processing in accordance with the terms of the Agreement and this Addendum.

III. Twilio as a Processor - Processing Customer Content

5. Customer Instructions. Customer appoints Twilio as a processor to process Customer Content on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this Addendum, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents and preventing spam or fraudulent activity, and detecting and preventing network exploits and abuse); (b) as necessary to comply with applicable law; and (c) as otherwise agreed in writing by the parties ("*Permitted Purposes*").

5.1 Lawfulness of Instructions.Customer will ensure that its instructions comply with Applicable Data Protection Law. Customer acknowledges that Twilio is not responsible for determining which laws are applicable to Customer's business nor whether Twilio's provision of the Services meets or will meet the requirements of such laws. Customer will ensure that Twilio's processing of Customer Content, when done in accordance with Customer's instructions, will not cause Twilio to violate any applicable law, regulation, or rule, including Applicable Data Protection Law. Twilio will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate any applicable law, regulation, or rule, including Applicable Data Protection Law.

5.2 Additional Instructions. Additional instructions outside the scope of the Agreement, an Order Form, or this Addendum will be agreed to between the parties in writing, including any additional fees that may be payable by Customer to Twilio for carrying out those instructions.

6. Confidentiality.

6.1 Responding to Third Party Requests. In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory authority, or third party is made directly to Twilio in connection with Twilio's processing of Customer Content, Twilio will promptly inform Customer and provide details of the same, to the extent legally permitted. Unless legally obligated to do so, Twilio will not respond to any such request, inquiry, or complaint without Customer's prior consent except to confirm that the request relates to Customer.

6.2 Confidentiality Obligations of Twilio Personnel.Twilio will ensure that any person it authorizes to process the Customer Content has agreed to protect personal data in accordance with Twilio's confidentiality obligations under the Agreement.

7. Sub-processing.

7.1 Sub-processors. Customer agrees that Twilio may use sub-processors to fulfill its contractual obligations under the Agreement. Where Twilio authorizes any sub-processor as described in this Section 7, Twilio agrees to impose data protection terms on any sub-processor it appoints that require it to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.

7.2 General Consent for Onward Sub-processing. Customer provides a general consent for Twilio to engage onward sub-processors, conditional on the following requirements:

(a) Any onward sub-processor must agree in writing to only process data in a country that the European Commission has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses, or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities; and

(b) Twilio will restrict the onward sub-processor's access to personal data only to what is strictly necessary to provide the Services, and Twilio will prohibit the sub-processor from processing the personal data for any other purpose.

7.3 Current Sub-processors and Notification of New Sub-processors. If Twilio Ireland Limited or Twilio Japan G.K. is the Twilio party to the Agreement, then Customer consents to Twilio engaging Twilio Inc. as a sub-processor, which has its primary processing facilities in the United States of America. Customer consents to Twilio engaging additional third party sub-processors to process Customer Content within the Services for the Permitted Purposes provided that Twilio maintains an up-to-date list of its sub-processors at https://www.twilio.com/legal/sub-processors (https://www.twilio.com/legal/sub-processors), which contains a mechanism for Customer to subscribe to notifications of new sub-processors. If Customer subscribes to such notifications, Twilio will provide details of any change in sub-processors as soon as reasonably practicable. With respect to changes in infrastructure providers, Twilio will endeavor to give notice sixty (60) days prior to any change, but in any event will give notice no less than thirty (30) days prior to any such change. With respect to Twilio's other sub-processors, Twilio will endeavor to give notice thirty (30) days prior to any change, but will give notice no less than ten (10) days prior to any such change.

7.4 Objection Right for new Sub-processors. Customer may object to Twilio's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such event, the parties agree to discuss commercial reasonable alternative solutions in good faith. If the parties cannot reach a resolution within ninety (90) days, Customer may suspend or terminate the affected service in accordance with the termination provisions of the Agreement. Such termination will be without prejudice to any fees incurred by Customer prior to suspension or termination. If no objection has been raised prior to Twilio replacing or appointing a new sub-processor, Twilio will deem Customer to have authorized the new sub-processor.

7.5 Sub-processor Liability. Twilio will remain liable for any breach of this Addendum that is caused by an act, error or omission of its sub-processors.

8. Data Subject Rights.

8.1 Twilio Services. As part of the Twilio Services, Twilio provides Customer with a number of self-service features, including the ability to delete, obtain a copy of, or restrict use of Customer Content, which may be used by Customer to assist in complying with its obligations under Applicable Data Protection Law with

respect to responding to requests from data subjects via the Twilio Services at no additional cost. In addition, upon Customer's request, Twilio will provide reasonable additional and timely assistance (at Customer's expense only if complying with the Customer's request will require Twilio to assign significant resources to that effort) to assist Customer in complying with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

8.2 SendGrid Services. Twilio will, taking into account the nature of the processing, provide reasonable assistance to Customer to the extent possible to enable Customer to respond to requests from a data subject seeking to exercise its rights under Applicable Data Protection Law with respect to Customer Content being processed via the SendGrid Services.

9. Impact Assessments and Consultations. Twilio will provide reasonable cooperation to Customer in connection with any data protection impact assessment (at Customer's expense only if such reasonable cooperation will require Twilio to assign significant resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Law.

10. Return or Deletion of Customer Content. Twilio will, in accordance with Section 2 of Schedule 1 (Details of Processing), delete or return to Customer any Customer Content stored in the Services.

10.1 Extension of Addendum. Upon termination of the Agreement, Twilio may retain Customer Content in storage for the time periods set forth in Schedule 1 (Details of Processing), provided that Twilio will ensure that Customer Content is processed only as necessary for the Permitted Purposes, and Customer Content remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

10.2 Retention Required by Law. Notwithstanding anything to the contrary in this Section 10, Twilio may retain Customer Content or any portion of it if required by applicable law, provided that it remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

IV. Security and Audits

11. Security

11.1 Security Measures. Twilio has implemented and will maintain the technical and organizational measures set out in the Security Controls to protect personal data from a Security Incident. Additional information about the technical and organizational security measures involving (a) the Twilio Services are described at https://www.twilio.com/security (https://www.twilio.com/security) and (b) the SendGrid Services are described at https://sendgrid.com/policies/security (https://sendgrid.com/policies/security).

11.2 Determination of Security Requirements. Customer acknowledges that the Services include certain features and functionalities that Customer may elect to use that impact the security of the data processed by Customer's use of the Services, such as, but not limited to, encryption of voice recordings and availability of multi-factor authentication on Customer's Services account or optional TLS encryption within the SendGrid Services. Customer is responsible for reviewing the information Twilio makes available regarding its data security, including its audit reports, and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations, including its obligations under Applicable Data Protection Law. Customer is further responsible for properly configuring the Services and using features and functionalities made available by Twilio to maintain appropriate security in light of the nature of the data processed by Customer's use of the Services.

11.3 Security Incident Notification. Twilio will provide notification of a Security Incident in the following manner:

a. Twilio will, to the extent permitted by applicable law, notify Customer without undue delay, but in no event later than seventy-two (72) hours after, Twilio's confirmation or reasonable suspicion of a Security Incident impacting Customer Data of which Twilio is a processor;

b. Twilio will, to the extent permitted and required by applicable law, notify Customer without undue delay of any Security Incident involving Customer Data of which Twilio is a controller; and

c. Twilio will notify the email address of Customer's account owner.

Twilio will make reasonable efforts to identify and, to the extent such Security Incident is caused by a violation of the requirements of this Addendum by Twilio, remediate the cause of such Security Incident. Twilio will provide reasonable assistance to Customer in the event that Customer is required under Applicable Data Protection Law to notify a regulatory authority or any data subjects of a Security Incident.

12. Audits. The parties acknowledge that Customer must be able to assess Twilio's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as Twilio is acting as a processor on behalf of Customer.

12.1 Twilio's Audit Program. Twilio uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Content. Such audits are performed at least once annually at Twilio's expense by independent third party security professionals at Twilio's selection and result in the generation of a confidential audit report ("*Audit Report*"). A description of Twilio's certifications and/or standards for audit of the (a) Twilio Services can be found at https://www.twilio.com/security (https://www.twilio.com/security); and (b) SendGrid Services can be found at https://sendgrid.com/policies/security (https://sendgrid.com/policies/security/).

12.2 Customer Audit. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Twilio will make available to Customer a copy of Twilio's most recent Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Law (including, where applicable, Article 28(3) of the GDPR or Clauses 5(f) and 12(2) of the Standard Contractual Clauses) will be satisfied by these Audit Reports. To the extent that Twilio's provision of an Audit Report does not provide sufficient information or to the extent that Customer must respond to a regulatory authority audit, Customer agrees to a mutually agreed-upon audit plan with Twilio that: (a) ensures the use of an independent third party; (b) provides notice to Twilio in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Customer at Twilio's then-current rates unless Customer is on Twilio's Enterprise Edition; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Customer; and (g) obligates Customer, to the extent permitted by law, to keep confidential any information gathered that, by its nature, should be confidential.

V. International Provisions

13. Processing in the United States. Customer acknowledges that, as of the Effective Date, Twilio's primary processing facilities are in the United States of America.

14. Cross Border Data Transfer Mechanisms for Data Transfers. To the extent that Customer's use of the Services requires transfer of personal data out of the European Economic Area ("*EEA*"), Switzerland, or a jurisdiction set forth in Schedule 4, then Twilio will take such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law.

14.1 Order of Precedence. In the event that the Services are covered by more than one transfer mechanism, the transfer of personal data will be subject to a single transfer mechanism in accordance with the following order of precedence: (a) Twilio's binding corporate rules as set forth in Section 14.2 (Twilio BCRs - Twilio Services); (b) the Standard Contractual Clauses as set forth in Section 14.3 (Standard Contractual Clauses); and, if neither (a) or (b) are applicable, then (c) other applicable data transfer mechanisms permitted by Applicable Data Protection Law.

14.2 Twilio BCRs - Twilio Services. The parties agree that Twilio will process personal data in the Twilio Services in accordance with Twilio's Binding Corporate Rules as set forth at https://www.twilio.com/legal/binding-corporate-rules (https://www.twilio.com/legal/binding-corporate-rules) ("*Twilio BCRs*"). The parties further agree that, with respect to the Twilio Services, the Twilio BCRs will be the lawful transfer mechanism of Customer Account Data, Customer Content and Customer Usage Data from the EEA, Switzerland, or the United Kingdom to Twilio in the United States, or any other non-EEA Twilio entity subject to the binding corporate rules. For avoidance of doubt, the Twilio BCRs do not apply to SendGrid Services.

14.3 Standard Contractual Clauses. This Addendum hereby incorporates by reference (a) the Standard Contractual clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU, provided that Appendices 1 and 2 of the Standard Contractual Clauses shall be deemed completed as set forth in Schedule 2 to this Addendum; and (b) the Standard Contractual Clauses for data controller to data controller transfers approved by the European Commission in decision 2004/915/EC, provided that Annex B of the Standard Contractual Clauses shall be deemed completed as set forth in Schedule 3 to this Addendum. The parties further agree that the Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area, the United Kingdom, and/or Switzerland to outside the European Economic Area, the United Kingdom, and Switzerland, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission (or, in the case of transfers from the UK or Switzerland, the competent authority for the UK or Switzerland) as providing an adequate level of protection for personal data and (ii) not covered by the Twilio BCRs.

15. Jurisdiction Specific Terms. To the extent Twilio processes personal data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 4, then the terms specified in Schedule 4 with respect to the applicable jurisdiction(s) ("*Jurisdiction Specific Terms*") apply in addition to the terms of this Addendum. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will take precedence.

VI. Miscellaneous

16. Cooperation and Data Subject Rights. In the event that either party receives: (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) or (b) any other correspondence, enquiry, or complaint received from a data subject, regulator or other third party, (collectively, "*Correspondence*") then, where such Correspondence relates to processing of Customer Account Data or Customer Usage Data conducted by the other party, it will promptly inform such other party and the parties agree to cooperate in good faith as necessary to respond to such Correspondence and fulfill their respective obligations under Applicable Data Protection Law.

17. Sensitive Data. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing any Sensitive Data over the Services, or prior to permitting End Users to transmit or process Sensitive Data over the Services.

18. Notification Cooperation. Customer acknowledges that Twilio, as a controller, may be required by Applicable Data Protection Law to notify the regulatory authority of Security Incidents involving Customer Usage Data. If the regulatory authority requires Twilio to notify impacted data subjects with whom Twilio

does not have a direct relationship (e.g., Customer's end users), Twilio will notify Customer of this requirement. Customer will provide reasonable assistance to Twilio to notify the impacted data subjects.

19. GDPR Penalties. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

20. Conflict. If there is any conflict between this Addendum and the Agreement and/or Privacy Policy, then the terms of this Addendum will control. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

21. Failure to Perform. In the event that changes in law or regulation render performance of this Addendum impossible or commercially unreasonable, the Parties may renegotiate this Addendum in good faith. If renegotiation would not cure the impossibility, or the Parties cannot reach an agreement, the Parties may terminate the Agreement in accordance with the Agreement's termination provisions.

22. Updates. Twilio may update the terms of this Data Protection Addendum from time to time; provided, however, Twilio will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services.

SCHEDULE 1

DETAILS OF PROCESSING

1. Nature and Purpose of the Processing. Twilio will process personal data as necessary to provide the Services under the Agreement. Twilio does not sell Customer's personal data or Customer end users' personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

1.1 Customer Content. Twilio will process Customer Content in accordance with Section 5 (Customer Instructions) of this Addendum.

1.2 Customer Account Data. Twilio will process Customer Account Data as a controller (a) in order to manage the relationship with Customer; (b) carry out Twilio's core business operations, such as accounting and filing taxes; and (c) in order to detect, prevent, or investigate security incidents, fraud and other abuse and/or misuse of the Services.

1.3 Customer Usage Data. Twilio will process Customer Usage Data as a controller in order to carry out the necessary functions as a communications service provider, such as: (a) Twilio's accounting, tax, billing, audit, and compliance purposes; (b) to provide, optimize, and maintain the Services and platform and security; (c) to investigate fraud, spam, wrongful or unlawful use of the Services; and/or (d) as required by applicable law.

2. Duration of the Processing.

2.1 Customer Content.

a. Twilio Services. Prior to the termination of the Agreement, Twilio will process stored Customer Content for the Permitted Purposes until Customer elects to delete such Customer Content via the Twilio Services. Prior to the termination of the Agreement, Customer agrees that it is solely responsible for deleting Customer Content via the Twilio Services. Upon termination of the Agreement, Twilio will (i) provide Customer thirty (30) days after the termination effective date to obtain a copy of any stored Customer Content via the Twilio Services; (ii) automatically delete any stored Customer Content thirty (30) days after the termination effective date; and (iii) automatically delete any stored Customer Content on Twilio's back-up systems sixty (60) days after the termination effective date. Any Customer Content archived on Twilio's back-up systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law.

b. SendGrid Services. Upon termination of the Agreement, Twilio will (i) at Customer's election, delete or return to Customer the Customer Content (including copies) stored in the SendGrid Services and (ii) automatically delete any stored Customer Content on Twilio's back-up systems one (1) year after the termination effective date.

2.2 Customer Account Data. Twilio will process Customer Account Data as long as needed to provide the Services to Customer as required for Twilio's legitimate business needs, or as required by law. Customer Account Data will be stored in accordance with the Privacy Policy.

2.3 Customer Usage Data. Upon termination of the Agreement, Twilio may retain, use, and disclose Customer Usage Data for the purposes set forth in Section 1.3 of this Schedule 1, subject to the confidentiality obligations set forth in the Agreement. Twilio will anonymize or delete Customer Usage Data when Twilio no longer requires it for the purposes set forth in Section 1.3 of this Schedule 1.

3. Categories of Data Subjects.

3.1 Customer Content. Customer's end users.

3.2 Customer Account Data. Customer's employees and individuals authorized by Customer to access Customer's Twilio account or make use of Customer's telephone number assignments received from Twilio.

3.3 Customer Usage Data. Customer's end users.

4. Type of Personal Data. Twilio processes personal data contained in Customer Account Data, Customer Content, and Customer Usage Data as defined in the Addendum.

SCHEDULE 2

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix 1.

Data exporter

The data exporter is the Customer and the user of the Services.

Data importer

The data importer is Twilio Inc, a provider of (a) business communications services that enable communications features and capabilities to be embedded into web, desktop and mobile software applications; and (b) cloud-based transactional and marketing email delivery, management and analytics services.

Data subjects

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

Data exporter's end-users. The data importer will receive any personal data in the form of Customer Content that the data exporter instructs it to process through its cloud communications products and services. The precise personal data that the data exporter will transfer to the data importer is necessarily determined and controlled solely by the data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Customer Content: As defined in Section 1 (Definitions) of this Addendum.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Twilio does not intentionally collect or process any special categories of data in the provision of its products or services.

However, special categories of data may from time to time be processed through the Services where the data exporter or its end users choose to include this type of data within the communications it transmits using the Services. As such, the data exporter is solely responsible for ensuring the legality of any special categories of data it or its end users choose to process using the Services.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

For the Twilio Services, the provision of programmable communication products and services, primarily offered in the form of APIs, on behalf of the data exporter, including transmittal to or from data exporter's software application from or to the publicly-switched telephone network (PSTN) or by way of other communications networks.

For the SendGrid Services, the provision of products and services which allow the sending and delivering email communications on behalf of the data exporter to its recipients. Twilio will also provide the data exporter with analytic reports concerning the email communications it sends on the data exporter's behalf.

Storage on Twilio's network.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 2 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 documentation/legislation attached): See Security Controls.

SCHEDULE 3

ANNEX B TO THE STANDARD CONTRACTUAL CLAUSES

DESCRIPTION OF THE TRANSFER

This Annex B forms part of the Standard Contractual Clauses and must be completed and signed by the parties.

Data Subjects

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

Data exporter and data exporter's end users.

Purposes of the Transfer(s)

The transfer is made for the following purposes:

The provision of cloud communication services.

and

For provision of a portion of the Twilio Services under which data exporter adds an additional factor for verification of data exporter's end users' identity in connection with such end users' use of data exporter's software applications or services ("*2 Factor Authentication Services*").

Categories of data

The personal data transferred concern the following categories of data:

1. Personal data transferred by data exporter to data importer to provide 2 Factor Authentication Services, namely data subjects' telephone numbers and email addresses and any other personal data provided by the data exporter and/or needed for authentication purposes.
2. Customer Account Data: As defined in Section 1 (Definitions) of this Addendum.
3. Customer Usage Data: As defined in Section 1 (Definitions) of this Addendum.

Recipients

The personal data transferred may only be disclosed to the following recipients or categories of recipients:

- Employees, agents, affiliates, advisors and independent contractors of data importer with a reasonable business purpose for needing such personal data
- Vendors of data importer that, in their performance of their obligations to data importer, must process such personal data acting on behalf of and according to instructions from data importer.
- Any person (natural or legal) or organization to whom data importer may be required by applicable law or regulation to disclose personal data, including law enforcement authorities, central and local government.

Sensitive data

N/A

Data protection registration of the data exporter

_____

SCHEDULE 4

JURISDICTION SPECIFIC TERMS

1.Australia:

1.1. The definition of "Applicable Data Protection Law" includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2. The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Law.

1.3. The definition of "Sensitive Data" includes "Sensitive Information" as defined under Applicable Data Protection Law.

2. Brazil:

2.1 The definition of "Applicable Data Protection Law" includes the Lei Geral de Proteção de Dados (LGPD).

2.2 The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to the data subjects.

2.3 The definition of "processor" includes "operator" as defined under Applicable Data Protection Law.

3. California:

3.1 The definition of "Applicable Data Protection Law" includes the California Consumer Privacy Act (CCPA).

3.2 The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Law and, for clarity, includes any Personal Information contained within Customer Account Data, Customer Content, and Customer Usage Data.

3.3 The definition of "data subject" includes "Consumer" as defined under Applicable Data Protection Law. Any data subject rights, as described in Section 8 (Data Subject Rights) of this Addendum, apply to Consumer rights. In regards to data subject requests, Twilio can only verify a request from Customer and not from Customer's end user or any third party.

3.4 The definition of "controller" includes "Business" as defined under Applicable Data Protection Law.

3.5 The definition of "processor" includes "Service Provider" as defined under Applicable Data Protection Law.

3.6 Twilio will process, retain, use, and disclose personal data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Twilio agrees not to (a) sell (as defined by the CCPA) Customer's personal data or Customer end users' personal data; (b) retain, use, or disclose Customer's personal data for any commercial purpose (as defined by the CCPA) other than providing the Services; or (c) retain, use, or disclose Customer's personal data outside of the scope of the Agreement. Twilio understands its obligations under the Applicable Data Protection Law and will comply with them.

3.7 Twilio certifies that its sub-processors, as described in Section 7 (Sub-processing) of this Addendum, are Service Providers under Applicable Data Protection Law, with whom Twilio has entered into a written contract that includes terms substantially similar to this Addendum. Twilio conducts appropriate due diligence on its sub-processors.

3.8 Twilio will implement and maintain reasonable security procedures and practices appropriate to the nature of the personal data it processes as set forth in Section 11 (Security) of this Addendum.

4. Canada:

4.1. The definition of "Applicable Data Protection Law" includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).

4.2. Twilio's sub-processors, as described in Section 7 (Sub-processing) of this Addendum, are third parties under Applicable Data Protection Law, with whom Twilio has entered into a written contract that includes terms substantially similar to this Addendum. Twilio has conducted appropriate due diligence on its sub-processors.

4.3. Twilio will implement technical and organizational measures as set forth in Section 11 (Security) of this Addendum.

5. Israel:

5.1 The definition of "Applicable Data Protection Law" includes the Protection of Privacy Law (PPL).

5.2 The definition of "controller" includes "Database Owner" as defined under Applicable Data Protection Law.

5.3 The definition of "processor" includes "Holder" as defined under Applicable Data Protection Law.

5.4 Twilio will require that any personnel authorized to process Customer Content comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel sign confidentiality agreements with Twilio in accordance with Section 6 (Confidentiality) of this Addendum.

5.5 Twilio must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Section 11 (Security) of this Addendum and complying with the terms of the Agreement.

5.6 Twilio must ensure that the personal data will not be transferred to a sub-processor unless such sub-processor has executed an agreement with Twilio pursuant to Section 7.1 (Sub-processors) of this Addendum.

6. Japan:

6.1 The definition of "Applicable Data Protection Law" includes the Act on the Protection of Personal Information (APPI).

6.2 The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Law.

6.3 The definition of "controller" includes "Business Operator" as defined under Applicable Data Protection Law. As a Business Operator, Twilio is responsible for the handling of personal data in its possession.

6.4 The definition of "processor" includes a business operator entrusted by the Business Operator with the handling of personal data in whole or in part (also a "trustee"), as described under Applicable Data Protection Law. As a trustee, Twilio will ensure that the use of the entrusted personal data is securely controlled.

7. Mexico:

7.1. The definition of "Applicable Data Protection Law" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE).

7.2. When acting as a processor, Twilio will:

(a) treat personal data in accordance with Customer's instructions as outlined in in Section 5 (Customer Instructions) of this Addendum;

(b) process personal data only to the extent necessary to provide the Services;

(c) implement security measures in accordance with Applicable Data Protection Law and Section 11 (Security) of this Addendum;

(d) keep confidentiality regarding the personal data processed in accordance with the Agreement;

(e) delete all personal data upon termination of the Agreement in accordance with Section 10 (Return or Deletion of Customer Content) of this Addendum; and

(f) only transfer personal data to sub-processors in accordance with Section 7 (Sub-processing) of this Addendum.

8. Singapore:

8.1 The definition of "Applicable Data Protection Law" includes the Personal Data Protection Act 2012 (PDPA).

8.2 Twilio will process personal data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 11 (Security) of this Addendum and complying with the terms of the Agreement.

9. United Kingdom:

9.1 References in this Addendum to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018)

9.2 The Standard Contractual Clauses will also apply to Customer in the United Kingdom as data exporter and to Twilio as data importer for transfers of personal data to countries that are not deemed to have an adequate level of data protection under the United Kingdom's Applicable Data Protection Law.