DATA PROTECTION ADDENDUM

Binding Corporate Rules, CCPA, GDPR, Privacy Shield, and Standard Contractual

Revised July 2019

twilio

Once fully executed, this DPA forms a part of the agreement between Twilio and Customer for the provision of the SendGrid Services and Twilio Services. To complete this DPA, Customers should submit a request via the Twilio DPA request portal at https://ahoy.twilio.com/gdpr. Twilio will send a pre-signed copy of the DPA ready for execution, generally within one business day.

For questions about Twilio's DPA or how Twilio handles personal information, contact privacy@twilio.com.

Data Protection Addendum

This Data Protection Addendum ("***Addendum***") is entered into as of the date it is fully executed as indicated in the signature blocks below ("***Effective Date***"), and amends and supplements the Terms of Service, Master Sales Agreement or other written or electronic agreement between Twilio and Customer for the provision of the Services ("***Agreement***").

I. Introduction

1. Definitions.

- "***Applicable Data Protection Law***" refer to all laws and regulations applicable to Twilio's processing of personal data under the Agreement.
- "***controller***", "***processor***", "***data subject***", "***personal data***" and "***processing***" (and "***process***") have the meanings given in accordance with Applicable Data Protection Law;
- "***Customer***" shall mean the Customer entity that is a party to the Agreement.
- "***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 Twilio account and billing information of individuals that Customer has associated with its Twilio account.
- **"*Customer Content***" means (a) content exchanged by means of use of the Twilio Services, such as text, message bodies, voice and video media, images, and sound; (b) data stored on Customer's behalf via the Twilio Services such as communication logs; (c) personal data sent via the SendGrid Services such as sender, recipient, and copy recipient identification information (first and last name), contact information (address, telephone number (fixed and mobile), email address, fax number), employment information (job title); and (d) any other personal data that the Customer chooses to include within the body of an email that it sends using the SendGrid Services.
- "***Customer Usage Data***" means data processed by Twilio for the purposes of transmitting, distributing or exchanging Customer Content; including data used to trace and 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 Twilio

Services, and the date, time, duration and the type of communication; and (b) activity logs used to trace and identify the source of SendGrid Service requests, optimize and maintain performance of the SendGrid Services, and investigate and prevent system abuse.

- "***Privacy Policy***" means (a) for the Twilio Services, Twilio Inc.'s then-current privacy policy available at https://www.twilio.com/legal/privacy ("***Twilio's Privacy Policy***"); and (b) For the SendGrid Services, SendGrid, Inc.'s then-current privacy policy available at https://sendgrid.com/policies/privacy ("***SendGrid's Privacy Policy***").

- "***Privacy Shield Framework***" means the EU-US and/or Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.

- "***Privacy Shield Principles***" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles).

- "***SendGrid Services***" means the services provided by SendGrid, Inc. enabling companies to develop, transmit, analyze, and manage email communications and other related digital communications and tools through the SendGrid, Inc. proprietary website available to Customer (currently available at 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 SendGrid, Inc., excluding any Twilio Services.

- "***Sensitive Data***" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof), (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; (f) date of birth; (g) criminal history; (h) mother's maiden name; and (i) any other information that falls within the definition of "special categories of data" under Applicable Data Protection Law.

- "***Service Data***" means aggregated, non-personally identifiable data or information (data or information that does not identify an entity or natural person as the source thereof) resulting from Customer's and its End Users' use and operation of the SendGrid Services, including information relating to volumes, frequencies, bounce rates or any other information regarding the email and other communications Customer or its End Users generate and send using the SendGrid Services. For the avoidance of doubt, this Addendum will not apply to Service Data.

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

- "***Twilio***" means the Twilio entity or affiliate that is party to the Agreement, being Twilio Inc., a company incorporated in the state of Delaware; Twilio Ireland Limited ("***Twilio Ireland***"), a company incorporated in the country of Ireland; Twilio Japan G.K. ("***Twilio Japan***"), a company incorporated in the country of Japan, and/or SendGrid, Inc., a corporation incorporated in the state of Delaware.

- "***Twilio Services***" means the cloud software platform and other services offered and provided by Twilio Inc. to Customer under this Agreement, which are generally comprised of two components: (a) platform services, including the Twilio APIs and any cloud-based software provided to Customer by Twilio Inc. and training, support, programs, features, functions, developer tools, and report formats, and subsequent updates or upgrades of any of the foregoing made generally available by Twilio Inc., and (b) connectivity services, which include the interconnection capabilities embedded within the Twilio Services that link the Twilio Services to the telecommunication providers' networks (including fixed-line, cellular, wireless, high-bandwidth, and/or fiber optic cable) via the Internet. The Twilio Services excludes any SendGrid Services.

  Any capitalized term 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 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. Schedule 1 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. Twilio will process Customer Account Data, and Customer Usage Data in accordance with Applicable Data Protection Law and consistent with the Privacy Policy and the Agreement.

4. Compliance. Customer is responsible for ensuring that it has complied, and will continue to comply, with all Applicable Data Protection Laws in its use of the Services and its own processing of personal data, such as ensuring its end users are provided adequate notice of Twilio's processing activities, including with respect to Customer end user data for which Twilio acts as a controller and making available to end users a privacy notice that fulfills the requirements of Applicable Data Protection Law; and 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 as set forth in the Agreement and this Addendum, as otherwise necessary to provide the Services (which may include investigating security incidents and preventing spam or fraudulent activity, and detecting and preventing network exploits and abuse), as necessary to comply with applicable law, or as otherwise agreed in writing ("***Permitted Purposes***").

5.1 Lawfulness of Instructions. Customer will ensure that its instructions comply with all laws applicable to the Customer Content, including without limitation, Applicable Data Protection Law. Customer will ensure that Twilio's processing of the Customer Content in accordance with Customer's instructions will not cause Twilio to violate any applicable law, regulation, or rule, including, without limitation, Applicable Data Protection Law. Twilio will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate Applicable Data Protection Law.

5.2 Resellers. If Customer is reselling the Services under the Agreement to third parties, then the terms set forth in Schedule 5 will apply.

5.3 Additional Instructions. Additional instructions outside the scope of the Agreement, Order Form, or this Addendum may result in additional fees 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 this Addendum. 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.

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, or pursuant to a compliant US-EU Privacy Shield certification; 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 Twilio Services Current Sub-processors and Notification of New Sub-processors. If Twilio Ireland or Twilio Japan 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 Inc. maintains an up-to-date list of its sub-processors for the Twilio Services at https://www.twilio.com/legal/sub-processors and SendGrid, Inc. does the same for the SendGrid services at https://sendgrid.com/policies/privacy/sub-processors, which each contain 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 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 a sub-processor, Twilio will deem Customer to have authorized the new sub-processors.

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, retrieve, 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 Customer's Twilio account or by using the applicable Twilio API at no additional cost. In addition, upon request, Twilio will provide reasonable additional and timely assistance (at Customer's expense) 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 their rights under EU Data Protection Legislation with respect to personal data 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) or consultations with supervisory authorities that may be required in accordance with Applicable Data Protection Law.

10. Return or Deletion of Customer Content.

10.1 Twilio Services. Twilio provides Customer the ability to obtain a copy of and delete Customer Content via the Twilio Services. Customer agrees that it is solely responsible for obtaining a copy of and deleting Customer Content via the Twilio Services. Upon termination of the Agreement, Twilio will (a) provide Customer thirty (30) days after the termination effective date to obtain a copy of any stored Customer Content via the Twilio Services; (b) automatically delete any stored Customer Content thirty (30) days after the termination effective date; and (c) 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.

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

10.3 Extension of Addendum. Upon termination of the Agreement, Twilio may retain Customer Content in storage for the periods stated in Sections 10.1 and 10.2, provided

that Twilio will ensure that Customer Content is processed only as necessary for the purpose specified in this Addendum and no other purpose, and Customer Content remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

10.4 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.

IV. Security and Audits

11. **Security Measures.** Twilio has implemented and will maintain appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to such data (a "***Security Incident***"). Measures to protect Customer Content from a Security Incident involving (a) the Twilio Services are described at https://www.twilio.com/security; and (b) the SendGrid Services are described at https://sendgrid.com/policies/security.

11.1 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 and this Addendum. Customer is further responsible for properly configuring the Services and using available features and functionalities to maintain appropriate security in light of the nature of the data processed by Customer's use of the Services.

11.2 Security Incident Notification — Customer Content: Twilio will, to the extent permitted by applicable law, notify Customer without undue delay via the email address of Customer's Twilio account owner of any Security Incident involving Customer Content of which Twilio becomes aware. To the extent such Security Incident is caused by a violation of the requirements of this Addendum by Twilio, Twilio will make reasonable efforts to identify and 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 supervisory authority or any data subjects of a Security Incident.

11.3 Security Incident Notification — Customer Usage Data: If Twilio becomes aware of a Security Incident involving Customer Usage Data containing the personal data of data subjects with whom Twilio does not have a direct relationship (e.g., Customer's end users) and Twilio determines that the incident must be reported to a regulatory authority, Twilio will notify the Customer of the incident and of its obligation and intent to notify the regulatory authority. If the impacted data subjects are required to be notified of a Security Incident under Applicable Data Protection Law, Customer will provide reasonable assistance to Twilio to effectuate appropriate notice to the impacted data subjects.

12. **Audits. The parties acknowledge that Customer must be able to assess Twilio's compliance with its obligations under Applicable Data Protection Law, 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; and (b) SendGrid Services can be found 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, and will only arise 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 or supervisory authority audit. In such event, Customer agrees to a mutually agreed-upon audit plan that: ensures the use of an independent third party; provides notice to Twilio in a timely fashion; requests access only during business hours; accepts billing to Customer at Twilio's then-current rates unless Customer is on Twilio's Enterprise

Edition; occurs no more than once annually; restricts its findings to only data relevant to Customer; and obligates Customer to, to the extent permitted by law, keep confidential any information gathered that, by its nature, should be confidential.

V. International Provisions

13. **Processing in the United States and Other Locations.** Customer acknowledges that, as of the Effective Date of this Addendum, Twilio Inc. and SendGrid, Inc.'s primary processing facilities are in the United States of America. The SendGrid Services also use data centers in the United Kingdom, India, and Japan for geo-forwarding.

14. **Cross Border Data Transfer Mechanisms for Data Transfers.** To the extent that Customer's use of the Twilio 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; (b) EU-US and Swiss-US Privacy Shield Framework self-certifications as set forth in Section 14.3; and (c) the Standard Contractual Clauses as set forth in Section 14.4.

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 ("***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 Inc. in the United States, or any other non-EEA Twilio entity subject to the binding corporate rules

14.3 Privacy Shield. To the extent Twilio processes (or causes to be processed) any personal data via the Services originating from the EEA, Switzerland, or the United Kingdom, Twilio Inc. and SendGrid, Inc. represent that they are self-certified to the Privacy Shield Framework and agree that they will comply with the Privacy Shield Principles

when handling any such data. To the extent that Customer is (a) located in the United States of America and is also self-certified to the Privacy Shield or (b) located in the EEA, Switzerland or United Kingdom, Twilio Inc. and SendGrid, Inc. further agree to (i) provide at least the same level of protection to such data as is required by the Privacy Shield Principles; (ii) notify Customer without undue delay if its self-certification to the Privacy Shield is withdrawn, terminated, revoked, or otherwise invalidated and to cooperate in good faith to put in place such alternative data export mechanisms as are required under Applicable Data Protection Law; and (iii) upon notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of personal data.

14.4 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 2010/593/EU, provided that Appendices 1 and 2 of the Standard Contractual Clauses are 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 are 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 and/or Switzerland to outside the European Economic Area, United Kingdom, and Switzerland, either directly or via onward transfer, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive) and (b) not covered by the Twilio BCRs or by the Privacy Shield certification.

15. Jurisdiction Specific Terms. To the extent Twilio processes personal data originating from and protected by Applicable Data Protection Laws 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 in connection with the processing of the Customer Account Data and Customer Usage Data, (collectively, "***Correspondence***") then, where such Correspondence relates to processing 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. Prohibited Data. Customer will not transmit (or cause to be transmitted) any Sensitive Data via the SendGrid Services for processing under the Agreement, and Twilio will have no liability whatsoever for Sensitive Data sent via the SendGrid Services, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this Addendum will not apply to Sensitive Data when sent via the SendGrid Services.

18. 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.

19. GDPR Penaltiest. 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. Material Change in Law. If any modification to this Addendum is required to comply with a material change in Applicable Data Protection Law ("***Material Law Change***"), then either party may notify the other party in writing and propose modifications, and the parties may renegotiate the terms of this Addendum, in good faith, solely for the purpose of complying with a Material Law Change. If such renegotiation does not render terms that comply with a Material Change in Law, or, the parties cannot reach an agreement, then the parties may

mutually agree to terminate the Agreement.

21. Entire Agreement; Conflict. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Twilio and Customer. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is any conflict between this Addendum and any agreement, including the Agreement, then the terms of this Addendum will control. Any claims brought under this Addendum will be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

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 end users' information with third parties for compensation or for those third parties' own business interests.

   1.1 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.

   1.2 Customer Usage Data. Twilio will process Customer Usage Data as a controller in order to carry out necessary functions as a communications service provider including, but not limited to, (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 (c) as required by applicable law.

   1.3 Customer Content. Twilio will process Customer Content in accordance with Section 5 of the Addendum.

2. Duration of the Processing.

   2.1 Customer Account Data. Twilio will process Customer Account Data as long as needed to provide the Services to Customer. Customer Account Data stored in Twilio's relationship management system(s) is generally stored for up to seven years following termination of the Agreement. Invoice and billing records may be retained for longer periods for accounting, tax, and audit purposes depending on and in accordance with applicable law. Customer Account Data stored in communications with Twilio's Customer Support Teams may be retained for up to three years after termination of the Agreement. Apart from the above, within sixty (60) days following termination of the Agreement, Twilio will delete or anonymize personal data contained in Customer Account Data.

   2.2 Customer Content. Twilio will process Customer Content as outlined in Section 10 of the Addendum.

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 1.2 of this Schedule, subject to the confidentiality obligations set forth in the Agreement. Twilio will anonymize or otherwise delete Customer Usage Data when Twilio no longer requires it for the foregoing purposes.

3. Categories of Data Subjects.

3.1 Customer Account Data. Customer's employees and individuals authorized by Customer to access Customer's Twilio account.

3.2 Customer Content. Customer's customers and end-users.

3.3 Customer Usage Data. Customer's customers and 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

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

Data exporter

The data exporter is the Customer as defined above and the user of Twilio Inc.'s services and/or SendGrid, Inc.'s services.

Data importer

The data importer for the Twilio Services is Twilio Inc., a provider of business communications services that enable communications features and capabilities to be embedded into web, desktop and mobile software applications.

The data importer for the SendGrid Services is SendGrid, Inc., a provider of 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 customers and 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 above.

Special categories of data (if appropriate)

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

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

However, special categories of data may from time to time be inadvertently processed by Twilio Inc. where the data exporter or its end users choose to include this type of data within the communications it transmits using Twilio Inc.'s products and/or 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 Twilio Inc.'s products and/or services.

SendGrid, Inc. does not collect or process any special categories of data in the provision of its products and/or 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. SendGrid, Inc. 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 forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or documentation/legislation attached):

See https://www.twilio.com/security for information and details regarding technical and organisational measures regarding the Twilio Services.

See https://sendgrid.com/policies/security for information and details regarding technical and organisational measures regarding the SendGrid Services.

Schedule 3

ANNEX B TO THE STANDARD CONTRACTUAL CLAUSES

DESCRIPTION OF THE TRANSFER

This Appendix forms part of the 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 customers and 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 add an additional factor for verification of data exporter's customers' and end users' identity in connection with such customers' and 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 above.

3. Customer Usage Data: As defined above.

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 pursuant 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. California:

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

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

2.3 The definition of "data subject" includes "Consumer" as defined under Applicable Data Protection Law. Any Data Subject Rights, as described in Section 8 of the 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.

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

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

2.6 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 sell Customer's personal data or Customer end users' personal data; retain, use, or disclose Customer's personal data for any commercial purpose other than providing the Services; or 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.

2.7 Twilio certifies that its sub-processors, as described in Section 7 of the 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.

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

3. Canada:

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

3.2 Twilio's sub-processors, as described in Section 7 of the 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.

3.3 Twilio will implement technical and organizational measures as set forth in Section 11 of the Addendum.

4. Chile:

4.1 The definition of "Applicable Data Protection Law" includes Law 19.628.

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 of the 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 of the 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 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.

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 Section 5 of the 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 of the 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 of the Addendum; and

f. only transfer personal data to sub-processors in accordance with Section 7 of the 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 of the Addendum and complying with the terms of the Agreement.

9. United Kingdom:

9.1 The definition of "Applicable Data Protection Law" includes the Data Protection Act 2018.

Schedule 5

RESELLER TERMS

If Customer is reselling the Services under the Agreement to third parties (each third party, a "Reseller Customer"), the following terms apply:

1. Reseller Instructions. Customer instructs Twilio to process Reseller Customers' Customer Content provided by Customer on behalf of, and in accordance with, Reseller Customer instructions as necessary to provide the Services to the instructing Reseller Customer and support for the Services (if applicable) to the instructing Reseller Customer, or as otherwise agreed to in writing between Customer and Twilio. Customer will ensure that Reseller Customer instructions comply with all laws, regulations, and rules applicable to the Customer Content, and that Twilio's processing of the Customer Content in accordance with Reseller Customer's instructions will not cause Twilio to violate any applicable law, regulation, or rule, including Applicable Data Protection Law. Reseller Customer must not provide instruction to Twilio regarding the suspension or closure of accounts on the Service, and Twilio will not be obligated to comply with any such instruction.
2. Conflicting Instructions Between Reseller Customer and Customer. In the event Reseller Customer instructs Twilio to process data in a manner which contradicts Customer's instruction (each, a "Conflicting Instruction"), Twilio will comply with Customer's instruction. Twilio will have no liability for failure to comply with Conflicting Instructions and Customer will be responsible for resolving any dispute with Reseller Customer arising from Twilio's non-compliance with any Conflicting Instruction.