Data Protection Addendum

Last Updated: August 1, 2022

This Data Protection Addendum ("*Addendum*") forms part of the agreement between Customer and Twilio covering Customer's use of the Services (as defined below) ("*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.
- "*controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "*Customer Account Data*" means personal data that relates to Customer's relationship with Twilio, including the names 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 (including providing the MFA Services, as defined below), or as part of its legal obligation to retain Subscriber Records (as defined below).

- "*Customer Content*" means (a) personal data exchanged as a result of using the Services (as defined below), such as text message bodies, voice and video media, images, email bodies, email recipients, sound, and, where applicable, details Customer submits to the Services from its designated software applications and services and (b) data stored on Customer's behalf such as communication logs within the Services or marketing campaign data that Customer has uploaded to the Services (as defined below).
- "*Customer Data*" has the meaning given in the Agreement. Customer Data includes Customer Account Data, Customer Usage Data, Customer Content, and Sensitive Data, each as defined in this Addendum.
- "*Customer Usage Data*" means data processed by Twilio for the purposes of transmitting or exchanging Customer Content utilizing phone numbers either through the Public Switched Telephone Network (PSTN) or by way of other communication networks. Customer Usage Data includes 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.
- "*Multi Factor Authentication Services*" or "*MFA Services*" means the provision of a portion of the Services under which Customer adds an additional factor for verification of Customer's end users' identity in connection with such end users' use of Customer's software applications or services.
- "*personal data*" means any information relating to an identified or identifiable natural person ("*data subject*"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "*processor*" means the entity which processes personal data on behalf of the controller.
- "*processing*" (and "*process*") means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- "*Security Incident*" means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

- "*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), financial information, banking account numbers or passwords; (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, mother's maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of "special categories of data" under GDPR or any other applicable law or regulation relating to privacy and data protection.
- "*Services*" means the products and services provided by Twilio or its Affiliates, as applicable, that are (a) used by Customer, including, without limitation, products and services that are on a trial basis or otherwise free of charge or (b) ordered by Customer under an Order Form. Services include products and services that provide both (x) platform services, including access to any application programming interface ("*Twilio API*") and (y) where applicable, communications services used in connection with the Twilio APIs.
- *"Subscriber Records*" means Customer Account Data containing proof of identification and proof of physical address necessary for Twilio to provide Customer or Customer's end users with phone numbers in certain countries ("*telephone number assignments*"). When required by law or regulation, Subscriber Records are shared with local telecommunications providers, which provide local connectivity services, or local government authorities (additional information about these regulatory requirements is available at https://www.twilio.com/guidelines/regulatory (https://www.twilio.com/guidelines/regulatory)).
- "*sub-processor"* means (a) Twilio, when Twilio is processing Customer Content and where Customer is a processor of such Customer Content or (b) any third-party processor engaged by Twilio to process Customer Content in order to provide the Services to Customer. For the avoidance of doubt, telecommunication providers are not sub-processors.
- "*Third Party Request*" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.
- "*Twilio Privacy Notice"* means the privacy notice for the Services, the current version of which is available at https://www.twilio.com/legal/privacy (https://www.twilio.com/legal/privacy).

Capitalized terms not defined in this Section 1 will have the meaning given to them in this Addendum or 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. Twilio will process Customer Content in accordance with Customer's instructions as set forth in Section 5 (Customer Instructions).

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. Twilio will process Customer Account Data as a controller in order to (a) manage the relationship with Customer; (b) carry out Twilio's core business operations, such as accounting and filing taxes; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) perform identity verification; (e) comply with Twilio's legal or regulatory obligation to retain Subscriber Records; and (f) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the Twilio Privacy Notice.

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. 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, platform and security; (c) to investigate fraud, spam, wrongful or unlawful use of the Services; (d) as required by applicable law or regulation; or (e) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the Twilio Privacy Notice.

3. Purpose Limitation. Twilio will process personal data in order to provide the Services in accordance with the Agreement. Schedule 1 (Details of Processing) of this Addendum further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and categories of data subjects.

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, 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, and which includes investigating security incidents and preventing spam, fraudulent activity, and violations of the Twilio Acceptable Use Policy, the current version of which is available at https://www.twilio.com/legal/aup (https://www.twilio.com/legal/aup), and detecting and preventing network exploits or abuse; (b) as necessary to comply with applicable law or regulation, including Applicable Data Protection Law; and (c) as otherwise agreed in writing between 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 neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Twilio's provision of the Services meets or will meet the requirements of such laws or regulations. 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 or regulation, including Applicable Data Protection Law. Twilio will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate any applicable law or regulation, including Applicable Data Protection Law.

5.2 Additional Instructions. Additional instructions outside the scope of the Agreement 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 such additional instructions.

6. Confidentiality

6.1 Responding to Third Party Requests. In the event any Third Party Request 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. Twilio will not respond to any Third Party Request without Customer's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Customer.

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

7. Sub-processors

7.1 Authorization for Onward Sub-processing. Customer provides a general authorization for Twilio to engage onward sub-processors that is conditioned on the following requirements:

(a) Twilio will restrict the onward sub-processor's access to Customer Content 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;

(b) Twilio agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Content to the standard required by Applicable Data Protection

the requirements set forth in Schedule 4 (Jurisdiction Specific Terms) of this Addendum; and

(c) Twilio will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its sub-processors.

7.2 Current Sub-processors and Notification of Sub-processor Changes. Customer consents to Twilio engaging 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 written notice sixty (60) days prior to any change, but in any event will give written 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 written notice thirty (30) days prior to any change, but will give written notice no less than ten (10) days prior to any such change.

7.3 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 an event, the parties agree to discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach a resolution within ninety (90) days from the date of Twilio's receipt of Customer's written objection, Customer may discontinue the use of the affected Services by providing written notice to Twilio. Such discontinuation will be without prejudice to any fees incurred by Customer prior to the discontinuation of the affected Services. 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.

8. Data Subject Rights. As part of the 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. Customer may use these self-service features to assist in complying with its obligations under Applicable Data Protectio

respect to responding to requests from data subjects via the Services at no additional cost. To the extent Customer does not have the ability to resolve a data subject request through the self-service features, upon Customer's request, Twilio will provide reasonable additional and timely assistance to assist Customer in complying with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

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 3 (Duration of the Processing) of Schedule 1 (Details of Processing) of this Addendum, delete or return to Customer any Customer Content stored within 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) of this Addendum, provided that Twilio will ensure that Customer Content (a) is processed only as necessary for the Permitted Purposes and (b) 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 or regulation, including Applicable Data Protection Law, provided such Customer Content 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 security measures as set forth in the Agreement. Additional information about Twilio's technical and organizational security measures to protect Customer Data is set forth in Schedule 2 (Technical and Organizational Security Measures) of this Addendum.

11.2 Determination of Security Requirements. Customer acknowledges the Services include certain features and functionalities that Customer may elect to use which impact the security of Customer Data processed by Customer's use of the Services, such as, but not limited to, encryption of voice recordings, availability of multi-factor authentication on Customer's account, or optional Transport Layer Security (TLS) encryption. 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 Customer Data processed as a result of 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 discovery 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 Customer of any Security Incident via email to the email address(es) designated by Customer in Customer's account.

Twilio will make reasonable efforts to identify a Security Incident, and to the extent a Security Incident is caused by Twilio's violation of this Addendum, 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 impacted by 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*").

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 will be satisfied by these Audit Reports. To the extent that Twilio's provision of an Audit Report does not provide sufficient information or Customer is required to 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 written 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; (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 or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

V. International Provisions

13. 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 (Jurisdiction Specific Terms) of this Addendum, the terms specified in Schedule 4 with respect to the applicable jurisdiction(s) apply in addition to the terms of this Addendum.

14. Cross Border Data Transfer Mechanisms for Data Transfers. To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area, the United Kingdom, Switzerland, or any other jurisdiction listed in Schedule 4 (Jurisdiction Specific Terms) of this Addendum) to Twilio located outside of that jurisdiction ("*Transfer Mechanism*"), the terms set forth in Schedule 3 (Cross Border Transfer Mechanisms) of this Addendum will apply.

VI. Miscellaneous

15. 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 Third Party Request relating to the processing of Customer Account Data or Customer Usage Data conducted by the other party, such party will promptly inform such other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Law.

16. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Schedule 4 (Jurisdiction Specific Terms) of this Addendum; (2) the terms of this Addendum outside of Schedule 4 (Jurisdiction Specific Terms); (3) the Agreement; and (4) the Twilio Privacy Notice. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, without limitation, the exclusions and limitations set forth in the Agreement.

17. Updates. Twilio may update the terms of this 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. The then-current terms of this Addendum are available at https://www.twilio.com/legal/data-protection-addendum (https://www.twilio.com/legal/data-protection-addendum).

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 as a processor in accordance with Customer's instructions as set forth in Section 5 (Customer Instructions) of this Addendum.

1.2 Customer Account Data. Twilio will process Customer Account Data as a controller for the purposes set forth in Section 2.2 (Twilio as a Controller of Customer Account Data) of this Addendum.

1.3 Customer Usage Data. Twilio will process Customer Usage Data as a controller for the purposes set forth in Section 2.3 (Twilio as a Controller of Customer Usage Data) of this Addendum.

2. Processing Activities.

2.1 Customer Content. Personal data contained in Customer Content will be subject to the following basic processing activities:

(a) the provision of programmable communication products and services, primarily offered in the form of application programming interfaces (APIs), to Customer, including transmittal to or from Customer's software applications or; services and designated third parties as directed by Customer, from or to the publicly-switched telephone network (PSTN) or by way of other communications networks. Storage of personal data on Twilio's network.

(b) the provision of products and services which allow the transmission and delivery of email communications on behalf of Customer to its recipients. Twilio will also provide Customer with analytic reports regarding the email communications it sends on Customer's behalf. Storage of personal data on Twilio's network.

(c) the provision of products and services which allows Customer to integrate, manage and control its data relating to end users. Storage of personal data on Twilio's network.

2.2 Customer Account Data. Personal data contained in Customer Account Data will be subject to the processing activities of providing the Services.

2.3 Customer Usage Data. Personal data contained in Customer Usage Data will be subject to the processing activities of providing the Services.

3. Duration of the Processing. The period for which personal data will be retained and the criteria used to determine that period is as follows:

3.1 Customer Content.

(a) Services. Prior to the termination of the Agreement, (x) Twilio will process stored Customer Content for the Permitted Purposes until Customer elects to delete such Customer Content via the Services and (y) Customer agrees that it is solely responsible for deleting Customer Content via the Services. Except as set forth in Section 3.1(b) (SendGrid Services) of this Schedule 1, 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 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 or regulation.

(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 within any services and application programming interfaces branded as "SendGrid" or "Twilio SendGrid" (collectively, "*SendGrid Services*") and (ii) automatically delete any stored Customer Content in the SendGrid Services on Twilio's back-up systems one (1) year after the termination effective date.

3.2 Customer Account Data. Twilio will process Customer Account Data as long as required (a) to provide the Services to Customer; (b) for Twilio's legitimate business needs; or (c) by applicable law or regulation. Customer Account Data will be stored in accordance with the Twilio Privacy Notice.

3.3 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 (Customer Usage Data) 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 (Customer Usage Data) of this Schedule 1.

4. Categories of Data Subjects.

4.1 Customer Content. Customer's end users.

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

4.3 Customer Usage Data. Customer's end users.

5. Categories of Personal Data. Twilio processes personal data contained in Customer Account Data, Customer Content, and Customer Usage Data.

6. Sensitive Data or Special Categories of Data.

6.1 Customer Content. Sensitive Data may, from time to time, be processed via the Services where Customer or its end users choose to include Sensitive Data within the communications that are transmitted using the Services. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Customer's end users to transmit or process, any Sensitive Data via the Services.

6.2 Customer Account Data and Customer Usage Data.

(a) Sensitive Data may be found in Customer Account Data in the form of Subscriber Records containing passport or similar identifier data necessarily processed in order to receive telephone number assignments.

(b) Customer Usage Data does not contain Sensitive Data.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

The full text of Twilio's technical and organizational security measures to protect Customer Data is available at https://www.twilio.com/legal/security-overview (https://www.twilio.com/legal/security-overview) ("*Security Overview*").

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

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data	See Section 13 (Encryption) of the Security Overview (https://www.twilio.com/legal/security-overview)

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	See Section 18 (Resilience and Service Continuity) and Section 19 (Customer Data Backups) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	See Section 18 (Resilience and Service Continuity) and Section 19 (Customer Data Backups) of the Security Overview (https://www.twilio.com/legal/security-overview)

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	See Section 3 (Security Organization and Program), Section 7 (Security Certifications and Attestations), and Section 15 (Penetration Testing) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for user identification and authorisation	See Section 11 (Access Controls) of of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for the protection of data during transmission	See Section 13 (Encryption) and Section 19 (Customer Data Backups) of the Security Overview (https://www.twilio.com/legal/security-overview)

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures for the protection of data during storage	See Section 8 (Hosting Architecture and Data Segregation) and Section 13 (Encryption) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for ensuring physical security of locations at which personal data are processed	See Section 9 (Physical Security) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for ensuring events logging	See: https://www.twilio.com/docs/runtime/serverless-api/api/logs (https://www.twilio.com/docs/runtime/serverless-api/api/logs) and: https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed (https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed)

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures for ensuring system configuration, including default configuration	See: https://www.twilio.com/docs/runtime/serverless-api/api/logs (https://www.twilio.com/docs/runtime/serverless-api/api/logs) and: https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed (https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed)
Measures for internal IT and IT security governance and management	See Section 3 (Security Organization and Program) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for certification/assurance of processes and products	See Section 3 (Security Organization and Program) and Section 7 (Security Certifications and Attestations) of the Security Overview (https://www.twilio.com/legal/security-overview)

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures for ensuring data minimisation	As an organization, Twilio has adopted Binding Corporate Rules (https://www.twilio.com/legal/bcr) (BCRs) as the "code of conduct" for Twilio's processing of personal data worldwide. BCRs are based on the data protection principles of the GDPR. Twilio's BCRs were approved in May 2018 by European Union data protection authorities, and Twilio audits against and re-certifies its commitments established in its BCRs on an annual basis. More information about how Twilio processes personal data is set forth in the Privacy Policy available at https://www.twilio.com/legal/privacy (https://www.twilio.com/legal/privacy#twilio-privacy-statement), and further detailed in Twilio BCRs available at https://www.twilio.com/legal/bcr (https://www.twilio.com/legal/bcr).
Measures for ensuring data quality	As an organization, Twilio has adopted Binding Corporate Rules (https://www.twilio.com/legal/bcr) (BCRs) as the "code of conduct" for Twilio's processing of personal data worldwide. BCRs are based on the data protection principles of the GDPR. Twilio's BCRs were approved in May 2018 by European Union data protection authorities, and Twilio audits against and re-certifies its commitments established in its BCRs on an annual basis. More information about how Twilio processes personal data is set forth in the Privacy Policy available at https://www.twilio.com/legal/privacy (https://www.twilio.com/legal/privacy#twilio-privacy-statement), and further detailed in Twilio's BCRs available at https://www.twilio.com/legal/bcr (https://www.twilio.com/legal/bcr).

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures for ensuring limited data retention	As an organization, Twilio has adopted Binding Corporate Rules (https://www.twilio.com/legal/bcr) (BCRs) as the "code of conduct" for Twilio's processing of personal data worldwide. BCRs are based on the data protection principles of the GDPR. Twilio's BCRs were approved in May 2018 by European Union data protection authorities, and Twilio audits against and re-certifies its commitments established in its BCRs on an annual basis. More information about how Twilio processes personal data is set forth in the Privacy Policy available at https://www.twilio.com/legal/privacy (https://www.twilio.com/legal/privacy#twilio-privacy-statement), and further detailed in Twilio's BCRs available at https://www.twilio.com/legal/bcr (https://www.twilio.com/legal/bcr).
Measures for ensuring accountability	As an organization, Twilio has adopted Binding Corporate Rules (https://www.twilio.com/legal/bcr) (BCRs) as the "code of conduct" for Twilio's processing of personal data worldwide. BCRs are based on the data protection principles of the GDPR. Twilio's BCRs were approved in May 2018 by European Union data protection authorities, and Twilio audits against and re-certifies its commitments established in its BCRs on an annual basis. More information about how Twilio processes personal data is set forth in the Privacy Policy available at https://www.twilio.com/legal/privacy (https://www.twilio.com/legal/privacy#twilio-privacy-statement), and further detailed in Twilio's BCRs available at https://www.twilio.com/legal/bcr (https://www.twilio.com/legal/bcr).

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures for allowing data portability and ensuring erasure	Customer is able to export or delete Customer Content using the self-service features of the Services as set forth in the applicable documentation for the Services available at https://www.twilio.com/docs (https://www.twilio.com/docs). For an example of data portability self-service features, see: https://support.twilio.com/hc/en-us/articles/223183588-Exporting-SMS-and-Call-Logs (https://support.twilio.com/hc/en-us/articles/223183588-Exporting-SMS-and-Call-Logs) For an example of data portability self-service features, see: https://docs.sendgrid.com/ui/managing-contacts/create-and-manage-contacts#export-contacts (https://docs.sendgrid.com/ui/managing-contacts/create-and-manage-contacts#export-contacts) For an example of data erasure self-service features, see: https://support.twilio.com/hc/en-us/articles/223181008-Twilio-SMS-message-and-traffic-storage (https://support.twilio.com/hc/en-us/articles/223181008-Twilio-SMS-message-and-traffic-storage)

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
	For an example of data erasure self-service features, see: https://docs.sendgrid.com/api-reference/contacts/delete-contacts (https://docs.sendgrid.com/api-reference/contacts/delete-contacts)

Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, Twilio and the sub-processor enter into an agreement with data protection obligations substantially similar to those contained in this Addendum. Each sub-processor agreement must ensure that Twilio is able to meet its obligations to Customer. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify Twilio in the event of a Security Incident so Twilio may notify Customer; (b) delete personal data when instructed by Twilio in accordance with Customer's instructions to Twilio; (c) not engage additional sub-processors without Twilio's authorization; d) not change the location where personal data is processed; or (e) process personal data in a manner which conflicts with Customer's instructions to Twilio.

SCHEDULE 3

CROSS BORDER DATA TRANSFER MECHANISMS

1. Definitions

- "*BCR Services*" means all Services except the SendGrid Services.
- "*EEA*" means the European Economic Area
- "*EU Standard Contractual Clauses*" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
- "*Twilio BCRs*" means 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).
- "*UK International Data Transfer Agreement*" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.

2.1 Order of Precedence. In the event 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 2.2 (Twilio BCRs) of this Schedule 3; (b) the EU Standard Contractual Clauses as set forth in Section 2.3 (EU Standard Contractual Clauses) of this Schedule 3; (c) the UK International Data Transfer Agreement as set forth in Section 2.4 (UK International Data Transfer Agreement) of this Schedule 3; and, if neither (a) nor (b) nor (c) is applicable, then (d) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

2.2 Twilio BCRs. The parties agree that Twilio will process personal data within the BCR Services in accordance with the Twilio BCRs. The parties further agree that, with respect to the BCR 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 (a) Twilio in the United States of America or (b) any other non-EEA Twilio entity. For avoidance of doubt, the Twilio BCRs do not serve as a Transfer Mechanism for the SendGrid Services.

2.3 EU Standard Contractual Clauses. The parties agree that the EU Standard Contractual Clauses will apply to personal data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is: (a) not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data and (b) not covered by the Twilio BCRs. For data transfers from the EEA that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) Module One (Controller to Controller) of the EU Standard Contractual Clauses will apply where (i) Twilio is processing Customer Account Data and (ii) Customer is a controller of Customer Usage Data and Twilio is processing Customer Usage Data;

(b) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a controller of Customer Content and Twilio is processing Customer Content;

(c) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Content and Twilio is processing Customer Content;

(d) Module Four (Processor to Controller) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Usage Data and Twilio processes Customer Usage Data; and

(e) For each Module, where applicable:

(i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

(ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in Section 7.2 (Current Sub-processors and Notification of Sub-processor Changes) of this Addendum;

(iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

(iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

(v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(vi) in Annex I, Part A of the EU Standard Contractual Clauses:

Data Exporter: Customer

Contact details: The email address(es) designated by Customer in Customer's account via its notification preferences.

Data Exporter Role: The Data Exporter's role is set forth in Section 2 (Relationship of the Parties) of this Addendum.

Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement.

Data Importer: Twilio Inc.

Contact details: Twilio Privacy Team - privacy@twilio.com

Data Importer Role: The Data Importer's role is set forth in Section 2 (Relationship of the Parties) of this Addendum.

Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement;

(vii) in Annex I, Part B of the EU Standard Contractual Clauses:

The categories of data subjects are set forth in Section 4 of Schedule 1 (Details of Processing) of this Addendum.

The Sensitive Data transferred is set forth in Section 6 of Schedule 1 (Details of Processing) of this Addendum.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is set forth in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The purpose of the processing is set forth in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The period for which the personal data will be retained is set forth in Section 3 of Schedule 1 (Details of Processing) of this Addendum.

For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth at https://www.twilio.com/legal/sub-processors (https://www.twilio.com/legal/sub-processors);

(viii) in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority; and

(ix) Schedule 2 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the EU Standard Contractual Clauses.

2.4 UK International Data Transfer Agreement. The parties agree that the UK International Data Transfer Agreement will apply to personal data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is: (a) not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data and (b) not covered by the Twilio BCRs. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information is located in Section 2.3 (e)(vi) of this Schedule 3.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.3 (EU Standard Contractual Clauses) of this Schedule 3.

(c) In Table 3 of the UK International Data Transfer Agreement:

1. The list of Parties is located in Section 2.3(e)(vi) of this Schedule 3.
2. The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Schedule 1 (Details of the Processing).
3. Annex II is located in Schedule 2 (Technical and Organizational Security Measures)
4. The list of sub-processors is located at https://www.twilio.com/legal/sub-processors (https://www.twilio.com/legal/sub-processors).

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.5 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, including Schedule 4 (Jurisdiction Specific Terms), the Agreement, or the Twilio Privacy Notice, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.

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 Da

2.2 The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to 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 set forth 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 set forth in Section 7 (Sub-processors) 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 set forth in Section 7 (Sub-processors) 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. European Economic Area (EEA):

5.1 The definition of "Applicable Data Protection Law" includes the General Data Protection Regulation (EU 2016/679) ("*GDPR*").

5.2 When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

(a) require any appointed sub-processor 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, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process personal data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

5.3 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.

5.4 Customer acknowledges that Twilio, as a controller, may be required under Applicable Data Protection Law to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a 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.

6. Israel:

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

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

6.3 The definition of "processor" includes "Holder" as defined under Applicable Data Protection

6.4 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.

6.5 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.

6.6 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 (Authorization for Onward Sub-processing) of this Addendum.

7. Japan:

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

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

7.3 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.

7.4 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 defined under Applicable Data Protection Law. As a trustee, Twilio will ensure that the use of the entrusted personal data is securely controlled.

8. Mexico:

8.1 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).

8.2 When acting as a processor, Twilio will:

(a) treat personal data in accordance with Customer's instructions set forth 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-processors) of this Addendum.

9. Singapore:

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

9.2 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.

10. Switzerland:

10.1 The definition of “Applicable Data Protection Law” includes the Swiss Federal Act on Data Protection, as revised (FADP).

10.2 When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

(a) require any appointed sub-processor 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, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that Switzerland has declared to have an “adequate” level of protection or (ii) only process personal data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

10.3 To the extent that personal data transfers from Switzerland are subject to the EU Standard Contractual Clauses in accordance with Section 2.3 of Schedule 3 (Cross Border Data Transfer Mechanisms), the following amendments will apply to the EU Standard Contractual Clauses:

(a) references to "EU Member State" and "Member State' will be interpreted to include Switzerland, and

(b) insofar as the transfer or onward transfers are subject to the FADP:

(i) references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP;

(ii) the "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

(iii) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be goverened by the laws of Switzerland; and

(iv) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

11. United Kingdom (UK):

11.1 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).

11.2 When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

(a) require any appointed sub-processor 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, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that the United Kingdom has declared to have an “adequate” level of protection or (ii) only process personal data on terms equivalent to the UK International Data Transfer Agreement or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

11.3 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 UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.

11.4 Customer acknowledges that Twilio, as a controller, may be required under Applicable Data Protection Law to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a 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.

DocuSigned by:
Emmy Hackett
F824F46BEA71411...
06 December 2022

Emmy Hackett

General Counsel

SHL Group Ltd