DATA PROTECTION ADDENDUM

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

Revised February 2019

twilio

Once fully executed, this DPA forms a part of the agreement between Twilio and Customer for the provision of the 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 Twilio Terms of Service, Master Sales Agreement or other written or electronic agreement between Twilio and Customer for the provision of the Twilio Services ("***Agreement***"). If there is any conflict between this Addendum and the Agreement regarding the parties' respective privacy and security obligations, then the provisions of this Addendum shall control.

I. Introduction

1. Definitions.

- "***controller***", "***processor***", "***data subject***", "***personal data***" and "***processing***" (and "***process***") shall have the meanings given pursuant to Applicable Data Protection Law;
- "***Applicable Data Protection Law***" shall mean all laws and regulations applicable to the processing of personal data under the Agreement, including regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("***General Data Protection Regulation***" or "***GDPR***").
- "***Customer***" shall mean the Customer entity that is a party to the Agreement.
- "***Customer Account Data***" shall mean 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 Usage Data***" shall mean 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 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.
- "***Customer Content***" shall mean (a) content exchanged by means of use of the Twilio Services,

such as text, message bodies, voice and video media, images, and sound, and (b) data stored on Customer's behalf such as communication logs.

- "***Privacy Policy***" means Twilio's then-current privacy policy available at https://www.twilio.com/legal/privacy.
- "***Privacy Shield Framework***" shall mean the EU-US and/or Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.
- "***Privacy Shield Principles***" shall mean the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles).
- "***Twilio***" shall mean the Twilio entity that is party to the Agreement.
- "***Twilio Services***" shall have the meaning provided in the Agreement.

Any capitalized term used herein that is not defined shall have the meaning provided to it in the Agreement.

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 be a controller or processor, as applicable, 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 is a controller or processor, as applicable, and Twilio is an independent controller, not a joint controller with Customer.

Each party shall comply with its obligations pursuant to Applicable Data Protection Law and this Addendum when processing personal data.

3. Details of the processing. The subject matter of Twilio's processing of personal data is the provision of the Twilio Services pursuant to the Agreement. The duration of the processing,

the nature and purpose of the processing, and the types of personal data and categories of data subjects processed pursuant to this Addendum are further specified in Exhibit 1 (Details of the Processing) to this Addendum.

II. Processing Customer Content

4. 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, order forms, this Addendum, and as otherwise necessary to provide the Twilio Services (for example, instruction via Twilio Services APIs), or as otherwise agreed in writing ("***Permitted Purposes***"). Additional instructions outside the scope of the Agreement, this Addendum, or as otherwise needed to provide the Twilio Services may result in additional fees payable by Customer to Twilio for carrying out those instructions. Customer shall ensure that its instructions comply with all laws applicable to the Customer Content, including without limitation, Applicable Data Protection Law. Customer shall 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 agrees not to access or use Customer Content, except as necessary to maintain or provide the Twilio Services, or as necessary to comply with the applicable law or other binding governmental order.

5. Resellers. If Customer is reselling the Twilio Services pursuant to the Agreement to third parties (each third party a "***Reseller Customer***"), the following terms apply:

5.1 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 Twilio Services to the instructing Reseller Customer and support for the Twilio Services (if applicable) to the instructing Reseller Customer, or as otherwise agreed to in writing between Customer and Twilio. Customer shall 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 shall not provide instruction to Twilio regarding the suspension or closure of Twilio accounts, and Twilio shall not be obligated to comply with any such instruction.

5.2 Conflicting Instructions. In the event Reseller Customer instructs Twilio to process data in a manner which contradicts Customer's instruction (each, a "***Conflicting Instruction***"), Twilio shall comply with Customer's instruction. Twilio shall have no liability for failure to comply with Conflicting Instructions and Customer shall be responsible for resolving any dispute with Reseller Customer arising from Twilio's non-compliance with any Conflicting Instruction.

6. 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 shall promptly inform Customer and provide details of the same, to the extent legally permitted. Unless legally obligated to do so, Twilio shall not respond to any such request, inquiry or complaint without Customer's prior consent except to confirm that the request relates to Customer to which Customer hereby agrees.

7. Confidentiality Obligations of Twilio Personnel. Twilio will ensure that any person it authorizes to process the Customer Content shall protect the Customer Content in accordance with Twilio's confidentiality obligations pursuant to the Agreement.

8. Twilio Services Sub-processors. If Twilio Ireland Limited 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 for Permitted Purposes provided that:

8.1 Twilio Inc. maintains an up-to-date list of its sub-processors at https://www.twilio.com/legal/sub-processors/, which shall contain a mechanism for Customer to subscribe to notifications of new sub-processors. If Customer subscribes to such notifications, Twilio shall provide details of any change in sub-processors as soon as reasonably practicable. With respect to changes in infrastructure providers, Twilio shall endeavor to give notice

sixty (60) days prior to any change, but shall give notice no less than thirty (30) days prior to any such change. With respect to Twilio's other sub-processors, Twilio shall endeavor to give notice thirty (30) days prior to any change, but shall give notice no less than ten (10) days prior to any such change;

8.2 Twilio imposes 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; and

8.3 Twilio remains liable for any breach of this Addendum that is caused by an act, error or omission of its 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 shall discuss commercial reasonably alternative solutions in good faith. If the parties cannot reach resolution, Twilio will either not appoint or replace the sub-processor or, if this is not possible, Customer may terminate the affected Twilio Service or order form (without prejudice to any fees incurred by Customer prior to suspension or termination).

9. Data Subject Rights. 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 pursuant to 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 pursuant to Applicable Data Protection Law.

10. Impact Assessments and Consultations. Twilio shall provide reasonable cooperation to Customer in connection with any data protection impact assessment (such assistance to be provided at Customer's expense) or consultations with supervisory authorities that may be required pursuant to Applicable Data Protection Law.

11. Return or Deletion of Customer Content. Twilio provides Customer the ability to obtain

a copy of and delete Customer Content via the Twilio Services. During the Term of the Agreement, Customer agrees that it is solely responsible for obtaining a copy of and deleting Customer Content via the Twilio Services. Any Customer Content archived on Twilio's back-up systems shall be securely isolated and protected from any further processing, except as otherwise required by applicable Law, and deleted thirty (30) days following Customer initiating the deletion of Customer Content via the Twilio Services. Upon termination of this Agreement, Twilio will (i) provide Customer thirty (30) days after the termination effective date to obtain a copy of any stored Customer Content via the Twilio Services; (ii) automatically delete any stored Customer Content thirty (30) days after the termination effective date; and (iii) automatically delete any stored Customer Content on Twilio's back-up systems sixty (60) days after the termination effective date. Notwithstanding anything to the contrary in this Section 11, Twilio may retain Customer Content or any portion thereof if required by applicable Law.

12. Audit Obligations.

12.1 Twilio's Audit Program: The parties acknowledge that Customer must be able to assess Twilio's compliance with its obligations pursuant to Applicable Data Protection Law, insofar as Twilio is acting as a processor on behalf of Customer. 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 list of Twilio's certifications and/or standards for audit as of the date of this Addendum can be found at https://www.twilio.com/security.

12.2 Customer Audit: Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Twilio shall make available to Customer a copy of Twilio's most recent Audit Report. Customer further agrees that any such Audit Report meet Customer's audit requirements, and Customer agrees to exercise any right it may have to conduct an inspection or audit (including pursuant to Standard Contractual Clauses, as applicable) by instruction to Twilio to carry out the audit described above in Section 12.1 (Twilio's Audit Program). If Customer wishes to change this instruction, then Customer must send a written request to Twilio specifying the requested change. If Twilio declines the request to change the instruction, Customer may terminate the Agreement and this Addendum. If

Customer has executed an Agreement (but excluding the Twilio Terms of Service) and wishes to conduct an on-site audit of Twilio's security program and privacy obligations pursuant to Applicable Data Protection Law with regard to the processing of Customer Content pursuant to the Agreement, such audit shall (a) be subject to a mutually agreed audit plan; (b) be carried out during regular business hours in a way not to be disruptive to normal business operations; (c) be billed to Customer at Twilio's then-current rates unless Customer is subscribed to Twilio's Enterprise Plan; and (d) occur no more than once annually or following notice of a Security Incident. If the Standard Contractual Clauses apply, nothing in this Section 12 (Audit Obligations) varies or modifies the Standard Contractual Clauses nor affects the supervisory authorities' or data subjects' rights pursuant to the Standard Contractual Clauses.

13. Violations of 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.

III. Processing Customer Account Data and Customer Usage Data

14. Purpose Limitation. Twilio shall process Customer Account Data and Customer Usage Data in accordance with Applicable Data Protection Law and consistent with Twilio's Privacy Policy and the Agreement.

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 pursuant to 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 shall promptly inform such other party and the parties shall cooperate in good faith as necessary to respond to such Correspondence and fulfil their respective obligations pursuant to Applicable Data Protection Law.

16. Transparency. To the extent required by Applicable Data Protection Law, Customer shall be responsible for 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 shall make available to end users a privacy policy that fulfills the requirements of Applicable Data Protection Law.

IV. Security

17. Security Measures. Twilio has implemented and will maintain appropriate technical and organizational measures to protect Customer Account Data, Customer Usage Data, and Customer Content from (a) accidental or unlawful destruction and (b) loss, alteration, unauthorized disclosure of, or access to such data (a "***Security Incident***"). Measures to protect Customer Content from a Security Incident are described at https://www.twilio.com/security.

17.1 Determination of Security Requirements: Customer acknowledges that the Twilio 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 Twilio Services, such as, but not limited to, encryption of voice recordings and availability of multi-factor authentication on Customer's Twilio account. 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 Twilio Services meet the Customer's requirements and legal obligations, including its obligations pursuant to Applicable Data Protection Law and this Addendum. Customer is further responsible for properly configuring the Twilio 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 Twilio Services.

17.2 Security Incident Notification - Customer Content: Twilio shall, to the extent permitted by applicable law, promptly notify Customer via the email address of Customer's Twilio account owner of any known or reasonably suspected 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 shall make reasonable

efforts to identify and remediate the cause of such Security Incident. Twilio shall provide reasonable assistance to Customer in the event that Customer is required pursuant to Applicable Data Protection Law to notify a supervisory authority or any data subjects of the Security Incident.

17.3 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 the Security Incident pursuant to Applicable Data Protection Law, Customer will provide reasonable assistance to Twilio to effectuate appropriate notice to the impacted data subjects.

V. International Transfers of Data

18. Customer acknowledges that, as of the Effective Date of this Addendum, Twilio Inc.'s primary processing facilities are in the United States of America. To the extent that Customer's use of the Twilio Services requires transfer of personal data out of the European Economic Area ("***EEA***"), then Twilio will take such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include, without limitation, transferring the personal data to a recipient (a) in a country that the European Commission has decided provides adequate protection for personal data; (b) that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law; or (c) that has executed Standard Contractual Clauses adopted or approved by the European Commission.

In the event that the Twilio 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: (i) Twilio's binding corporate rules as set forth at https://www.twilio.com/legal/binding-corporate-rules ("Twilio BCRs"); (ii) Twilio Inc.'s EU-US and Swiss-US Privacy Shield Framework self-certifications; and (iii) the Standard Contractual Clauses as set forth in Exhibits 2 and 3 attached hereto.

18.1 Twilio BCRs: The parties agree that Twilio will process personal data in accordance with Twilio's binding corporate rules. The parties further agree that the Twilio BCRs shall be the lawful transfer mechanism of Customer Account Data, Customer Content and Customer Usage Data from the EEA to Twilio Inc. in the United States, or any other non-EEA Twilio entity subject to the binding corporate rules.

18.2 Privacy Shield: The parties further agree that the Privacy Shield Framework will be the lawful transfer mechanism of personal data from the EEA or Switzerland to Twilio Inc. in the United States of America, only to the extent such transfer is not covered by the Twilio BCRs. Twilio Inc. represents that it is self-certified to the Privacy Shield Framework and agrees, with respect to Customer Account Data, Customer Content and Customer Usage Data that it shall comply with the Privacy Shield Principles when handling any such data. To the extent that Customer is (i) located in the United States of America and also self-certified to the Privacy Shield or (ii) located in the EEA or Switzerland, Twilio Inc. further agrees:

18.2.1 To provide at least the same level of protection to such data as is required by the Privacy Shield Principles;

18.2.2 To notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles; and

18.2.3 Upon notice, including pursuant to Section 18.2.2 above, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of personal data.

18.3 Standard Contractual Clauses: The parties further agree that the Standard Contractual Clauses will apply to personal data that is transferred from the European Economic Area and/or Switzerland to outside the European Economic area 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.

VI. Miscellaneous

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

20. 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. If there is any conflict between this Addendum and any agreement, including the Agreement, then the terms of this Addendum shall control.

EXHIBIT 1

Details of the Processing

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

1.1 Customer Account Data. Twilio will process Customer Account Data in accordance with Section 14 of the Addendum. Twilio processes 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 Twilio Services.

1.2 Customer Content. Twilio will process Customer Content in accordance with Section 4 of the Addendum.

1.3 Customer Usage Data. Twilio will process Customer Usage Data in accordance with Section 14 of the Addendum. Twilio processes 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 investigate fraud, spam, or unlawful use of the Twilio Services; (c) to make carrier interconnection payments and/or (d) as required by applicable law.

2. Duration of the Processing.

2.1 Customer Account Data. Twilio will process Customer Account Data as long as needed to provide the Twilio Services to Customer. Customer Account Data stored in Twilio's relationship management system(s) is generally stored for up to seven (7) 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 (3) 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 12 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 Exhibit, subject to the confidentiality obligations set forth in the Agreement. Twilio shall 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.

EXHIBIT 2

Standard Contractual Clauses

European Commission Decision C(2 0 1 0) 5 9 3
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data transfer agreement between

Customer who has executed the above Addendum,
hereafter "data exporter"

and

Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 USA
Tel.: (877) 889-4546; fax (415) 376-8596; email: privacy@twilio.com
hereinafter "data importer;"

each a "party"; together "the parties".

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b. 'the data exporter' means the controller who transfers the personal data;

c. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d. 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f. 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of

which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e. that it will ensure compliance with the security measures;

f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j. that it will ensure compliance with Clause 4(a) to (i).

---

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

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

d. that it will promptly notify the data exporter about:

e. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

f. any accidental or unauthorised access, and

g. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

---

[2]*This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision*

h. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

i. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

j. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

k. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

l. that the processing services by the subprocessor will be carried out in accordance with Clause 11; to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data

exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

3. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

4. x=If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   b. to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses . Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against

the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

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 entity identified as the "data exporter" in the Twilio Data Protection Agreement, and the user of Twilio Inc.'s services.

Data importer

The data importer 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.

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: content exchanged by means of use of Twilio's Services, such as text, message bodies, voice and video media, images, and sound

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.

Processing operations

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

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.

Storage on Twilio Inc.'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 implemented by Twilio.

Appendix 3 To The Standard Contractual Clauses

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

This Appendix does not vary or modify the Clauses. It sets out the parties' interpretation of their respective obligations under specific Clauses identified below. As permitted by Clause 10 of these Clauses, the purpose of the interpretations is to enable the parties to fulfil their obligations in practice.

Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the noncompliance ("Cure Period").
4. If after the Cure Period the data importer has not or cannot cure the noncompliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(j): Disclosure of sub-processor agreements:

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward sub-processor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to sub-processor confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any sub-processor it appoints to permit it to disclose the sub-processor agreement to data exporter.
3. Even where data importer cannot disclose a sub-processor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such sub-processing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including,

but not limited to, the exclusions and limitations set forth in data importer's Terms of Service in effect as of the date of execution of these Clauses or other written or electronic agreement for data exporter's use and purchase of data importer's products and services. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward sub-processing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward sub-processing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward sub-processors. Such consent is conditional on data importer's compliance with the requirements set out below, which collectively ensure that the onward sub-processor will provide adequate protection for the personal data that it processes:

   a. any onward sub-processor must agree in writing:

      i. to only process personal data in the European Economic Area or another country that the European Commission has formally declared to have an "adequate" level of protection in accordance with the requirements of EU Directive 95/46/EC; or

      ii. to process personal data on terms equivalent to these Clauses or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities and whose scope extends to transfers of personal data from the territories in which the data exporter is established; and

[3]Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses). [4]However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

b. data importer must restrict the onward sub-processor's access to personal data only to what is strictly necessary to perform its subcontracted data processing services to data importer (which shall be consistent with the instructions issued to data importer by data exporter) and data importer will prohibit the onward sub-processor from processing the personal data for any other purpose.

EXHIBIT 2

Standard Contractual Clauses

European Commission Decision C(2004) 5271
Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

This data transfer agreement is effective as of the date the Addendum is executed by Customer (the "**Effective Date**"), and is between

Customer who has executed the above Addendum,
hereinafter "data exporter"

and

Twilio Inc.
375 Beale Street, Suite 300, San Francisco, CA 94105, USA
Tel: 877-889-4546; Fax: 415-376-8596, email: privacy@twilio.com
hereinafter "data importer"
each a "party"; together "the parties"..

Definitions

For the purposes of the clauses:

c. personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

d. "the data exporter" shall mean the controller who transfers the personal data;

e. "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

f. "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a. The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b. It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c. It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d. It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e. It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data

subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a. It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b. It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c. It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d. It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e. It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f. At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g. Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h. It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data , or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: iii (the data processing principles set forth in Annex A)

By executing these Clauses, the data importer agrees to process the personal data in accordance with the option indicated above.

i. It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a. Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b. The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a. In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b. The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c. Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a. In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b. In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c. Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d. The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any

rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject,

and

ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

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

Data Subjects

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

The data exporter, 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 services pursuant to which data exporters 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. 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 Account Data");

3. 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 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 ("Customer Usage Data").

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

Contact points for data protection enquiries is provided in the above Addendu