Twilio's Binding Corporate Rules: Processor Policy

PART I: INTRODUCTION TO THIS PROCESSOR POLICY

Starting with Why – Why Do We Have This Policy?

Twilio's guiding principle when it comes to data protection is "No Shenanigans." "No Shenanigans" mean we are thoughtful about data protection, we comply with the law, and strive to be honest, direct and transparent when it comes to processing personal data. Twilio respects people's personal data and we demonstrate that respect, not just by what we say about data protection, but in how we treat the personal data with which we have been entrusted to process.

This Binding Corporate Rules: Processor Policy ("Processor Policy") establishes Twilio's approach to compliance with applicable data protection laws (and, in particular, European laws) when processing personal data on behalf of a third party controller.

Members of our group of companies that are bound by this Policy are listed in Appendix 1 (https://www.twilio.com/legal/bcr/processor#appendix-1) ("Group Members").

Scope of this Processor Policy

The standards described in the Processor Policy are worldwide standards that apply to all Group Members when processing any personal data as a processor under this Policy. Accordingly, this Processor Policy applies regardless of the origin of the personal data that we process, the country in which we process personal data, or the country in which a Group Member is established.

This Processor Policy applies in particular when we process personal data as a processor on behalf of a third party controller located in Europe, including when the personal data is transferred to a Group Member for processing outside of Europe. This Processor Policy applies regardless of whether our Group Members process personal data by manual or automated means.

For an explanation of some of the terms used in this Processor Policy, like "controller", "process", and "personal data", please see the section headed "Important terms used in this Processor Policy" below.

Types of personal data within the scope of this Processor Policy

This Processor Policy applies to all personal data that we process as a processor on behalf of a third party controller (referred to as the "Customer" in this Processor Policy), including personal data processed in the course of providing services to a customer or another Group Member – such as the content of voice, video, SMS and other communications that Twilio's Customers or their end-users send and receive via Twilio's API. When a Customer transfers personal data to us for processing in accordance with this Processor Policy, a copy of this Processor Policy shall be incorporated into the contract with that Customer.

Excluded Products

There may be certain Twilio products or services where Twilio processes personal data as a processor but which fall outside of the scope of this Policy ("Excluded Products"). The current list of Excluded Products is at Appendix 10 (https://www.twilio.com/legal/bcr/processor#appendix-10). The Processor Policy will not be incorporated into the contracts that we have with Customers of Excluded Products. We will nonetheless ensure that our processing of any personal data within the Excluded Products is in compliance with applicable data protection laws and when transferring any such personal data for processing outside of Europe that appropriate safeguards, such as the Privacy Shield or the European Commission's standard contractual clauses, are put in place in accordance with the General Data Protection Regulation.

Our collective responsibility to comply with this Processor Policy

All Group Members and their staff must comply with this Processor Policy when processing personal data as a processor on behalf of a Customer, irrespective of the country in which they or the Customer are located.

In particular, all Group Members who process personal data as a processor under this Policy must comply with:

- the rules set out in Part II (https://www.twilio.com/legal/bcr/processor#part-ii-our-obligations) of this Processor Policy;
- the practical commitments set out in Part III (https://www.twilio.com/legal/bcr/processor#part-iii-delivering-compliance-in-practice) of this Processor Policy;
- the third party beneficiary rights set out in Part IV (https://www.twilio.com/legal/bcr/processor#part-iv-third-party-beneficiary-rights); and
- the related policies and procedures appended in Part V (https://www.twilio.com/legal/bcr/processor#part-v-related-policies-and-procedures) of this Processor Policy.

Responsibility towards the Customer

As a data processor, Twilio will have a number of direct legal obligations under applicable data protection laws. In addition, however, the Customer will also pass certain data protection obligations on to Twilio in its contract appointing Twilio as its processor. If Twilio fails to comply with the terms of its processor appointment, this may put the Customer in breach of its applicable data protection laws and Customer may initiate proceedings against Twilio for breach of contract, resulting in the payment of compensation or other judicial remedies.

A Customer may enforce this Processor Policy against any Group Member that is in breach of it. Where a non-European Group Member (or a non-European third party processor appointed by a Group Member) processes personal data for which the Customer is a controller in breach of this Processor Policy, that Customer may enforce the Processor Policy against Twilio Ireland Limited. In such event, Twilio Ireland Limited will be responsible for demonstrating that such Group Member (or third party processor) is not responsible for the breach, or that no such breach took place.

When a Customer transfers personal data to a Group Member for processing in accordance with this Processor Policy, a copy of this Processor Policy shall be incorporated into the contract with that Customer. If a Customer chooses not to rely upon this Processor Policy when transferring personal data a Group Member outside Europe, that Customer is responsible for implementing other appropriate safeguards in accordance with applicable data protection laws.

Management commitment and consequences of non-compliance

Twilio's management is fully committed to ensuring that all Group Members and their staff comply with this Processor Policy at all times. This Processor Policy ensures that our Customers can trust that Twilio will process their personal data appropriately, fairly and lawfully, no matter where that data may be processed within the Twilio organization.

Further, non-compliance with this Processor Policy may cause Twilio to be subject to sanctions imposed by competent data protection authorities and courts, and may cause harm or distress to individuals whose personal data has not been protected in accordance with the standards described in this Processor Policy.

In recognition of the importance of trust to Twilio’s business and the gravity of the risks associated with violating that trust, staff members who do not comply with this Processor Policy will be subject to disciplinary action, up to and including dismissal.

Relationship with Twilio's Binding Corporate Rules: Controller Policy

This Processor Policy applies only to personal data that Twilio processes as a processor in order to provide a service to a Customer.

Twilio has a separate Binding Corporate Rules: Controller Policy that applies when it processes personal data as a controller (i.e. for its own purposes). When a Twilio Group Member processes personal data as a controller, it must comply with the Controller Policy (https://www.twilio.com/legal/bcr/controller).

In some situations, Group Members may act as both a controller and a processor. Where this is the case, they must comply both with this Controller Policy and also the Processor Policy as appropriate. If in any doubt which policy applies to you, please speak with the Privacy Team whose contact details are provided below.

Where will this Processor Policy be made available?

This Processor Policy is accessible on Twilio's website at www.twilio.com/legal/bcr/processor. (https://www.twilio.com/legal/bcr/processor)

Important terms used in this Processor Policy

For the purposes of this Processor Policy:

- the term applicable data protection laws includes the data protection laws in force in the territory in which the controller of the personal data is located. Where a Group Member processes personal data on behalf of a European controller under this Processor Policy, the term applicable data protection laws shall include the European data protection laws applicable to that controller (including Europe's General Data Protection Regulation, when applicable);
- the term controller means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. For example, Twilio is a controller of its HR records and CRM records;
- the term Controller Policy refers to Twilio's Binding Corporate Rules: Controller Policy, which is available at www.twilio.com/bcr/controller (https://www.twilio.com/legal/bcr/controller). The Controller Policy applies where Twilio processes personal data as a controller (i.e. for its own purposes);
- the term Customer refers to the third party controller on whose behalf Twilio processes personal data. It includes Twilio's third party customers, as well as Twilio Group Members, when we process personal data on their behalf in the course of providing data processing services to them.
    - the term Europe as used in this Policy refers to the Member States of the European Economic Area – that is, the Member States of the European Union plus Norway, Lichtenstein and Iceland.
- the term Group Member means the members of Twilio's group of companies listed in Appendix 1 (https://www.twilio.com/legal/bcr/processor#appendix-1);
- the term personal data means any information relating to an identified or identifiable natural person. 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- the term processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- the term processor means a natural or legal person which processes personal data on behalf of a controller. For example, Twilio is a processor of personal data contained in communications content data it processes on behalf of its Customers;
- the term Processor Policy refers to this Binding Corporate Rules: Processor Policy. The Processor Policy applies where Twilio processes personal data as a processor on behalf of a third party;
- the term special categories of data means information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also includes information about an individual's criminal offences or convictions, as well as any other information deemed sensitive under applicable data protection laws; and
- the term staff refers to all employees, new hires, individual contractors and consultants, and temporary staff engaged by any Twilio Group Member. All staff must comply with this Processor Policy.

How to raise questions or concerns

If you have any questions regarding this Processor Policy, your rights under this Processor Policy or applicable data protection laws, or any other data protection issues, you can contact Twilio's Privacy Team using the details below. Twilio's Privacy Team will either deal with the matter directly or forward it to the appropriate person or department within Twilio to respond.

Attention:	Privacy Team
Email:	privacy@twilio.com
Address:	375 Beale Street, Suite 300 San Francisco, CA 94105

Twilio's Privacy Team is responsible for ensuring that changes to this Policy are notified to the Group Members and to Customers whose personal data is processed by Twilio in accordance with Appendix 9 (https://www.twilio.com/legal/bcr/processor#appendix-9).

If you want to exercise any of your data protection rights, please see the data protection rights procedure set out in Appendix 2 (https://www.twilio.com/legal/bcr/processor#appendix-2). Alternatively, if If you are unhappy about the way in which Twilio has used your personal data, you can raise a complaint in accordance with our complaint handling procedure set out in Appendix 6 (https://www.twilio.com/legal/bcr/processor#appendix-6).

PART II: OUR OBLIGATIONS

This Processor Policy applies where a Group Member processes personal data as a processor anywhere in the world. All staff and Group Members must comply with the following obligations:

Rule 1 – Lawfulness:

We must ensure that processing is at all times compliant with applicable law and this Processor Policy.

We must at all times comply with any applicable data protection laws, as well as the standards set out in this Processor Policy, when processing personal data.

Accordingly:

- where applicable data protection laws exceed the standards set out in this Processor Policy, we must comply with those laws; but
- where there are no applicable data protection laws, or where applicable data protection laws do not meet the standards set out in this Processor Policy, we must process personal data in accordance with the standards set out in this Processor Policy.

Rule 2 – Cooperation with Customers:

We must cooperate with and assist the Customer to comply with its obligations under applicable data protection laws in a reasonable time and to the extent reasonably possible.

We must cooperate with and assist our Customers to comply with their obligations under applicable data protection laws. We must provide this assistance within a reasonable time and as required under the terms of our contract with the Customer. Assistance may include, for example, helping our Customer to keep the personal data we process on its behalf accurate and up to date, or helping it to provide individuals with access to their personal data, or helping it to conduct data protection impact assessments in accordance with applicable data protection laws.

Rule 3 – Fairness and transparency:

Our Customer has a duty to explain to the individuals whose data it processes (or instructs us to process), how and why that data will be used. This information must be

We must, to the extent reasonably possible, assist a Customer to comply with the requirement to explain to individuals how their personal data will be processed.

given in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

This is usually done by means of an easily accessible fair processing statement. We will provide assistance and information to the Customer in accordance with the terms of our contract with the Customer as required to assist them in complying with this requirement.

For example, the terms of our contract with a Customer may require us to provide information about any sub-processors we appoint to process personal data on our Customer's behalf.

Rule 4 – Purpose limitation:

Where we are acting as a processor, we will only process personal data on behalf of, and in accordance with the instructions of, the Customer.

Where we process personal data as a processor, we mu only process that personal data on behalf of the Custon and in accordance with its documented instructions (example, as set out in the terms of our contract with t Customer), including with regard to any internation transfers of personal data.

If we are unable to comply with our Customer's instructions (or any of our obligations under this Processor Policy), we will inform the Customer promptly. The Customer may then suspend its transfer of personal data to us and/or terminate its contract with us (in accordance with the terms of the contract).

In such circumstances, we will return, destroy or store the personal data, including any copies of the personal data, in a secure manner or as otherwise required, in accordance with the terms of our contract with the Customer and, if requested, certify to the Customer that this has been done.

If legislation prevents us from returning the personal data to our Customer, or from destroying it, we must inform the Customer. In such event, we must continue to maintain the confidentiality of the personal data and not actively process the personal data further other than in accordance with the terms of our contract with the Customer.

Rule 5 – Data accuracy and minimisation:

We must assist our Customer to comply with its obligation to keep personal data accurate and up to date. In particular, where a Customer informs us that personal

We will assist our Customer to keep the personal data accurate and up to date.

data is inaccurate, we must assist our Customer to update, correct or erase that data without undue delay.

We must also take measures to inform Group Members or third party processors to whom the personal data has been disclosed of the need to update, correct or erase that personal data.

Rule 6 – Storage limitation: We will assist our Customers to store personal data only for as long as is necessary for the purpose for which the information was initially collected.

Where a Customer instructs us that personal data we process on its behalf is no longer needed for the purposes for which it was collected, we will assist our Customer to erase, restrict or anonymise that personal data without undue delay and in accordance with the terms of our contract with the Customer. We must also take measures to inform Group Members or third party processors to whom the personal data has been disclosed of the need to erase, restrict or anonymise that personal data.

Rule 7 – Security, integrity and confidentiality:

We must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the personal data we process on behalf of a Customer.

Where we provide a service to a Customer which involves the processing of personal data, the contract between us and that Customer will set out the technical and organisational security measures we must implement to safeguard that data consistent with applicable data protection laws.

We must ensure that any staff member who has access to personal data processed on behalf of a Customer does so only for purposes that are consistent with the Customer's instructions and is subject to a duty of confidence.

Rule 8 – Security incident reporting:

We must notify a Customer of any security incident that we experience if it presents a risk to the personal data we process on the Customer's behalf.

When we become aware of a data security incident that presents a risk to the personal data that we process on behalf of a Customer, we must immediately inform the Privacy Team and follow our data security incident management policies.

The Privacy Team will review the nature and seriousness of the data security incident and determine whether it is necessary to notify a Customer. The Privacy Team shall be responsible for ensuring that any such notifications, where necessary, are made without undue delay and in accordance with applicable law.

We must obtain a Customer's authorisation before

Rule 9 – Engaging sub-processors:

We may only appoint, add or replace sub-processors with authorisation from the Customer and in accordance with its requirements.

appointing, adding or replacing a sub-processor to process personal data on its behalf. Authorisation must be obtained in accordance with the terms of our contract with the Customer.

We must make available to our Customer up-to-date information about the sub-processors we intend to appoint in order to obtain its authorisation. If, on reviewing this information, a Customer objects to the appointment of a sub-processor, that Customer may take such steps as are consistent with the terms of its contract with us and as referred to in Rule 4 of this Processor Policy regarding the return or destruction of the personal data.

Rule 10 – Sub-processor contracts:

We must only appoint sub-processors who protect personal data to a standard that is consistent with this Processor Policy and our contractual terms with Customers.

We must only appoint external sub-processors w[illegible] provide sufficient guarantees in respect of t[illegible] commitments made by us in this Processor Policy. In particular, external sub-processors must impleme[illegible] appropriate technical and organisational secur[illegible] measures to protect the personal data they process, and such measures must be consistent with our commitments to our Customer under our contractual terms with the Customer.

Where we intend to appoint an external sub-processor to process personal data, we must undertake due diligence to ensure it has in place appropriate technical and organisational security measures to protect the personal data. We must impose strict contractual obligations in writing on the sub-processor that require it:

- to protect the personal data to a standard that is consistent with our commitments to our Customer under the terms of our contract with the Customer;
- to maintain the security of the personal data, consistent with standards contained in this Processor Policy (and in particular Rules 7, 8 and above);
- to process personal data only on our instructions (which instructions will be consistent with the instructions of the Customer) or on the Customer's instructions; and
- to fulfil such additional obligations as may be necessary to ensure that the commitments made by the sub-processor reflect those made by us in this Processor Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of any international transfers of personal data.

Rule 11 – Respect for individuals' data protection rights:

We must assist our Customer to comply with its duty to respect the data protection rights of individuals, in accordance with the instructions of our Customer and the terms of our contract with the Customer.

We will assist a Customer to respond to queries or requests made by individuals in connection with their personal data.

In particular, if any Group Member receives a request from any individual wishing to exercise his or her data protection rights in respect of personal data for which the Customer is the controller, the Group Member must transfer such request promptly to the relevant Customer and not respond to such a request unless authorised to do so or required by law (in accordance with the Data Protection Rights Procedure in Appendix 2 (https://www.twilio.com/legal/bcr/processor#appendix-2)).

Rule 12 - Privacy by design and by default

We must provide our products and services in a way that assists our Customer to apply privacy by design and by default principles.

We must provide our products and services in a way tl assists our Customer to implement privacy by design a privacy by default principles. This means that we must implement appropriate technical and organizational measures when providing our products and services that: are designed to implement the data protection principles in an effective manner and to integrate the 57401187v1 18 necessary safeguards in order to protect the rights of individuals and meet the requirements of applicable data protection laws ("privacy by design"); and ensure that, by default, only personal data which are necessary for each specific processing purpose are collected, stored, processed and are accessible; in particular, that by default personal data is not made accessible to an indefinite number of people without the individual's intervention ("privacy by default"). These measures must be implemented in accordance with the terms of our agreement with our Customer.

PART III: DELIVERING COMPLIANCE IN PRACTICE

To ensure we follow the rules set out in our Processor Policy, in particular the obligations in Part II (https://www.twilio.com/legal/bcr/processor#part-ii-our-obligations), Twilio and all of its Group Members must also comply with the following practical commitments:

1. *Resourcing and compliance:*

Twilio has appointed its Privacy Team to oversee and ensure compliance with this Processor Policy. The Privacy Team is responsible for overseeing and enabling

We must have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

compliance with this Processor Policy on a day-to-day basis.

A summary of the roles and responsibilities of Twilio's Privacy Team is set out in Appendix 3 (https://www.twilio.com/legal/bcr/processor#appendix-3).

2. *Privacy training:*

We must ensure staff are educated about the need to protect personal data in accordance with this Processor Policy.

Group Members must provide appropriate privacy training to staff members who:

- have permanent or regular access to personal data; or
- are involved in the processing of personal data or in the development of tools used to process personal data

We will provide such training in accordance with t Privacy Training Program (see Appendix (https://www.twilio.com/legal/bcr/processor#append 4)).

3. Records of Data Processing We must maintain records of the data processing activities carried out on behalf of a Customer.

We must maintain a record of the processing activities that we conduct on behalf of a Customer in accordance with applicable data protection laws. These records should be kept in writing (including electronic form) and we must make these records available to competent data protection authorities upon request. The Privacy Team is responsible for ensuring that such records are maintained.

4. Audit:

We must have data protection audits on regular basis.

We will have data protection audits on a regular basis, which may be conducted by either internal or external accredited auditors. In addition, we will conduct data protection audits on specific request from the General Counsel and Chief Compliance Officer, the Privacy Team, the Audit Committee and/or the Board of Directors.

We will conduct any such audits in accordance with the Audit Protocol (see Appendix 5 (https://www.twilio.com/legal/bcr/processor#appendix-5)).

5. Complaint handling:

Group Members must enable individuals to raise data protection complaints and concerns (including complaints about processing under this Processor Policy) by

We must enable individuals to raise data protection complaints and concerns.

complying with the Complaint Handling Procedure (see Appendix 6 (https://www.twilio.com/legal/bcr/processor#appendix-6)).

6. Cooperation with competent data protection authorities:

We must always cooperate with competent data protection authorities.

Group Members must cooperate with competent data protection authorities by complying with the Cooperation Procedure (see Appendix 7 (https://www.twilio.com/legal/bcr/processor#appendix-7)).

7. Updates to this Processor Policy: We will update this Processor Policy in accordance with our Updating Procedure.

Whenever updating our Processor Policy, we must comply with the Updating Procedure (see Appendix 9 (https://www.twilio.com/legal/bcr/processor#append9)).

8. Conflicts between this Processor Policy and national legislation:

We must take care where local laws conflict with this Processor Policy, and act responsibly to ensure a high standard of protection for the personal data in such circumstances.

If local laws applicable to any Group Member prevents it from fulfilling its obligations under the Processor Policy or otherwise has a substantial effect on its ability to comply with the Processor Policy, or the instructions it has received from a Customer, the Group Member must promptly inform:

- the Customer (consistent with the requirements of Rule 4);
- the Privacy Team;
- the appropriate data protection authority competent for the Customer; and
- the appropriate data protection authority competent for the Group Member

unless otherwise prohibited by law.

9. Government requests for disclosure of personal data:

If a Group Member receives a legally binding request from a law enforcement authority or state security body for disclosure of personal data which is processed on behalf of an EEA Customer under this Processor Policy, it must:

- notify the EEA Customer promptly unless prohibited from doing so by a law enforcement authority or applicable law; and

We must comply with the Government Data Request Procedure in respect of a legally binding request for disclosure of personal data.

- use its best efforts to put the request on hold and notify the appropriate data protection authority competent for the EEA Customer by complying with the requirements of its Government Data Request Procedure set out in Appendix 9 (https://www.twilio.com/legal/bcr/processor#appendix-9).

In no event must transfers of personal data from a Group Member to any law enforcement, state security or similar public authority be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

PART IV: Third Party Beneficiary Rights

Application of this Part IV

This Part IV applies where individuals' personal data are protected under European data protection laws (including the General Data Protection Regulation). This is the case when:

- those individuals' personal data are processed in the context of the activities of a thirdparty controller or a Group Member (acting as processor) established in Europe;
- a non-European Customer (acting as controller) or Group Member (acting as processor) offers goods and services (including free goods and services) to those individuals in Europe; or
- a non-European Customer (acting as controller) or Group Member (acting as processor) monitors the behaviour of those individuals, as far as their behaviour takes place in Europe;

and that Customer or Group Member (as applicable) then transfers those individuals' personal data to a non-European Group Member (or its sub-processor) for processing under the Processor Policy.

Entitlement to effective remedies

When this Part IV applies, individuals have the right to pursue effective remedies in the event their personal data is processed by Twilio in breach of the following provisions of this Processor Policy:

- Part II (https://www.twilio.com/legal/bcr/processor#part-ii-our-obligations) (Our Obligations) of this Processor Policy;
- Paragraphs 5 (Complaints Handling), 6 (Cooperation with Competent Data Protection Authorities), 8 (Conflicts between this Processor Policy and national legislation) and 9 (Government requests for disclosure of personal data) under Part III of this Processor Policy; and
- Part IV (Third Party Beneficiary Rights) of this Processor Policy.

Individuals' third party beneficiary rights

When this Part IV applies, the right for individuals to pursue effective remedies against Twilio apply only if either (i) the requirements at stake are specifically directed at Twilio as a processor in accordance with applicable data protection law (and in accordance with the guidance published by competent data protection authorities), or (ii) the individuals cannot bring a claim against a Customer because:

- the Customer has factually disappeared or ceased to exist in law or has become insolvent; and
- no successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law.

In such cases, individuals may exercise the following rights:

- *Complaints*: Individuals may complain to a Group Member and/or to a European data protection authority, in accordance with the Complaints Handling Procedure at Appendix 7 (https://www.twilio.com/legal/bcr/processor#appendix-7);
- *Proceedings*: Individuals may commence proceedings against a Group Member for violations of this Processor Policy, in accordance with the Complaints Handling Procedure at Appendix 7 (https://www.twilio.com/legal/bcr/processor#appendix-7);
- *Compensation*: Individuals who have suffered material or non-material damage as a result of an infringement of this Processor Policy have the right to receive compensation from Twilio for the damage suffered.
- *Transparency*: Individuals also have the right to obtain a copy of the Processor Policy on request to the Privacy Team at privacy@twilio.com.

Responsibility for breaches by non-European Group Members

Twilio Ireland Limited will be responsible for ensuring that any action necessary is taken to remedy any breach of the Processor Policy by a non-European Group Member (or any nonEuropean sub-processor appointed by a Group Member).

In particular:

- If an individual can demonstrate damage it has suffered likely occurred because of a breach of this Processor Policy by a non-European Group Member (or a non-European sub-processor appointed by a Group Member), Twilio Ireland Limited will have the burden of proof to show that the non-European Group Member (or non-European subprocessor) is not responsible for the breach, or that no such breach took place.
- where a non-European Group Member (or any non-European third party sub-processor acting on behalf of a Group Member) fails to comply with this Processor Policy, individuals may exercise their rights and remedies above against Twilio Ireland Limited and, where appropriate, receive compensation (as determined by a competent court or other competent authority) from Twilio Ireland Limited for any material or non-material damage suffered as a result of a breach of this Processor Policy.

Shared liability for breaches with controllers

Where Twilio is engaged by a Customer to conduct processing and both are responsible for harm caused by the processing in breach of this Processor Policy, Twilio accepts that both Twilio and the Customer may be held liable for the entire damage in order to ensure effective compensation of the individual.

PART V: RELATED POLICIES AND PROCEDURES

Appendix 1

TWILIO GROUP MEMBERS

Part A: Twilio group members in the European Economic Area

	Name of entity	Registered address
1.	Twilio Estonia OU	Veerenni tn 38, Tallinn 11313, Estonia
2.	Twilio Germany GmbH	Rosenheimer Str. 143c 81671 Munich, Germany
3.	Twilio IP Holding Limited	25-28 North Wall Quay, Dublin 1, Ireland
4.	Twilio Ireland Limited	25-28 North Wall Quay, Dublin 1, Ireland
5.	Twilio Spain, S.L.	Calle Monte Esquinza 30, Bajo Izquierda, Madrid, 28010, Madrid, Espana
6.	Twilio Sweden AB	22 Södergatan, 211 15 Malmö, Sweden

7.	Twilio Berlin GmbH (f/k/a Core Network Dynamics GmbH)	Unter den Linden 10, 10117 Berlin, Germany
8.	Twilio Czechia a.s. (f/k/a ytica.com a.s.)	Sokolovská 694/100a, Karlin, Prague 8, Post Code 186 00, Czechia
9.	Twilio Netherlands B.V. (c/o TMF Netherlands B.V. / TMF Group)	Luna Arena, Herikerbergweg 238, 1101 CM Amsterdam, The Netherlands
10.	Twilio France SARL	c/o Primexis, Tour Pacific, 11-13 cours Valmy, 92977 Paris La Défense Cedex

Feedback

Part B. Twilio group members outside of the European Economic Area

	Name of entity	Registered address
1.	Twilio Australia Pty Ltd	c/o Baker McKenzie, Tower One - International Towers Sydney, Level 46, 100 Barangaroo Avenue, Barangaroo NSW 2000
2.	Twilio Canada Corp.	1600 - 925 West Georgia Street, Vancouver, BC V6C 3L2
3.	Twilio Colombia S.A.S	Calle 94 No. 11-30, P 2, Bogotá, Colombia
4.	Twilio Hong Kong Limited	c/o Baker McKenzie 14th Floor, One Taikoo Place 979 King's Road, Quarry Bay, SAR Hong Kong

5.	Twilio Inc.	101 Spear St Suite 300, San Francisco, CA 94105
6.	Twilio Japan G.K. (c/o ARK Outsourcing KK)	4-3-5-704 Ebisu, Shibuya-ku, Tokyo 150-0013, Japan
7.	Twilio ROW Ltd	C/O CML, Century House, 16 Par-la-Ville Road, Hamilton HM08, Bermuda
8.	Twilio Singapore Pte. Ltd	4 Shenton Way #28-03, SGX Centre II, Singapore 068807
9.	Teravoz Telecom Telecomunicacoes Ltda.	Rua Padra Joao Manuel, nº 808, 3º, Cerqueira Cesar, CEP 01411-000, São Paulo, Brazil
10.	Twilio Technology India Private Limited	GA, Alsa Glenridge, 32 Langford Road, Bengaluru, Karnataka 560025 India
11.	Twilio UK Limited	100 New Bridge Street, London, United Kingdom, EC4V 6JA

Appendix 2

DATA PROTECTION RIGHTS PROCEDURE

1. Introduction

1.1. Twilio's "Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the “Policies” or, respectively, the "Controller Policy"and the "Processor Policy") safeguard personal data transferred between the Twilio group members ("Group Members").

1.2. Individuals whose personal data are processed by Twilio under the Policies have certain data protection rights, which they may exercise by making a request to the controller of their information (whether the controller is Twilio or a Customer) (a"Data Protection Rights Request").

1.3. This Binding Corporate Rules: Data Protection Rights Procedure ("Procedure") describes how Twilio will respond to any Data Protection Rights Requests it receives from individuals whose personal data are processed and transferred under the Policies.

2. Individual's data protection rights

2.1. Twilio must assist individuals to exercise the following data protection rights, consistent with the requirements of applicable data protection laws:

a. The right of access: This is a right for an individual to obtain confirmation whether a controller processes personal data about them and, if so, to be provided with details of that personal data and access to it. This process for handling this type of request is described further in paragraph 4 below;

b. The right to rectification: This is a right for an individual to obtain rectification without undue delay of inaccurate personal data a controller may process about him or her. The process for handling this type of request is described further in paragraph 5 below.

c. The right to erasure: This is a right for an individual to require a controller to erase personal data about them on certain grounds – for example, where the personal data is no longer necessary to fulfil the purposes for which it was collected. The process for handling this type of request is described further in paragraph 5 below.

d. The right to restriction: This is a right for an individual to require a controller to restrict processing of personal data about them on certain grounds. The process for handling this type of request is described further in paragraph 5 below.

e. The right to object: This is a right for an individual to object, on grounds relating to his or her particular situation, to a controller's processing of personal data about him or her, if certain grounds apply. The process for handling this type of request is described further in paragraph 5 below.

f. The right to data portability: This is a right for an individual to receive personal data concerning him or her from a controller in a structured, commonly used and machine-readable format and to transmit that information to another controller, if certain grounds apply. The process for handling this type of request is described further in paragraph 6 below.

3. Responsibility to respond to a Data Protection Rights Request

3.1. Overview

3.1.1. The controller of an individual's personal data is primarily responsible for responding to a Data Protection Rights Request and for helping the individual concerned to exercise his or her rights under applicable data protection laws.

3.1.2. As such, when an individual contacts Twilio to make any Data Protection Rights Request then:

a. where Twilio is the controller of that individual's personal data under the Controller Policy, it must help the individual to exercise his or her data protection rights directly in accordance with this Procedure; and

b. where Twilio processes that individual's personal data as a processor on behalf of a Customer under the Processor Policy, Twilio must inform the relevant Customer promptly and provide it with reasonable assistance to help the individual to exercise his or her rights in accordance with the Customer's duties under applicable data protection laws.

3.2. Assessing responsibility to respond to a Data Protection Rights Request

3.2.1. If a Group Member receives a Data Protection Rights Request from an individual, it must pass the request to the Privacy Team at privacy@twilio.com immediately upon receipt indicating the date on which it was received together with any other information which may assist the Privacy Team to deal with the request.

3.2.2. The Privacy Team will make an initial assessment of the request as follows:

a. the Privacy Team will determine whether Twilio is a controller or processor of the personal data that is the subject of the request;

b. where the Privacy Team determines that Twilio is a controller of the personal data, it will then determine whether the request has been made validly under applicable data protection laws, whether an exemption applies (in accordance with section 3.4 below) and respond to the request (in accordance with section 3.5 below); and

c. where the Privacy Team determines that Twilio is a processor of the personal data on behalf of a Customer, it shall pass the request promptly to the relevant Customer in accordance with its contract terms with that Customer and will not respond to the request directly unless authorised to do so by the Customer.

3.3. Assessing the validity of a Data Protection Rights Request

3.3.1. If the Privacy Team determines that Twilio is the controller of the personal data that is the subject of the request, Twilio will then contact the individual in writing to confirm receipt of the Data Protection Rights Request.

3.3.2. A Data Protection Rights request must generally be made in writing, which can include email, unless applicable data protection laws allow a request to be made orally. A Data Protection Rights Request does not have to be official or mention data protection law to qualify as a valid request.

3.3.3. If Twilio has reasonable doubts concerning the identity of the individual making a request, it may request such additional information as is necessary to confirm the identity of the individual making the request. Twilio may also request any further information which is necessary to action the individual's request.

3.4. *Exemptions to a Data Rights Protection Rights Request*

3.4.1. Twilio will not refuse to act on Data Protection Rights Requests unless it can demonstrate that an exemption applies under applicable data protection laws.

3.4.2. Twilio may be exempt under applicable data protection laws from fulfilling the Data Protection Rights Request (or be permitted to charge a reasonable fee taking into account the administrative costs providing the information or communication or taking the action requested) if it can demonstrate that tl individual has made a manifestly unfounded or excessive request (in particular, because of the repetitive character of the request).

3.4.3. If Twilio decides not to take action on the Data Protection Rights Request, Twilio will inform the individual without delay and at the latest within one (1) month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the competent data protection authority and seeking a judicial remedy.

3.5. Responding to a Data Protection Rights Request

3.5.1. Where Twilio is the controller of the personal data that is the subject of the Data Protection Rights Request, and Twilio has already confirmed the identity of the requestor and has sufficient information to enable it to fulfil the request (and no exemption applies under applicable data protection laws), then Twilio shall deal with the Data Protection Rights Request in accordance with paragraph 4, 5 or 6 below (as appropriate).

3.5.2. Twilio will respond to a Data Protection Rights Request without undue delay and in no case later than one (1) month of receipt of that request. This one (1) month period may be extended by two (2) further months only if the request is complex or due to the number of requests that have been made.

4. Requests for access to personal data

4.1. Overview

4.1.1. An individual may require a controller to provide the following information concerning processing of his or her personal data:

a. confirmation as to whether the controller holds and is processing about that individual;

b. if so, a description of the personal purposes of the processing, the categories of personal data concerned, the envisaged period(s) (or the criteria used for determining those periods(s)) for which the personal data will be stored, and the recipients or categories of recipients to whom the information is, or may be, disclosed by the controller;

c. information about the individual's right to request rectification or erasure of his or her personal data or to restrict or object to its processing;

d. information about the individual's right to lodge a complaint with a competent data protection authority;

e. information about the source of the personal data if it was not collected from the individual;

f. details about whether the personal data is subject to automated decision-making (including automated decision-making based on profiling) which produces legal effects concerning the individual or similarly significantly affects them; and

g. where personal data is transferred from the European Economic Area to a country outside of the European Economic Area, the appropriate safeguards that Twilio has put in place relating to such transfers in accordance with applicable data protection laws.

4.1.2. An individual is also entitled to request a copy of his or her personal data from the controller. Where an individual makes such a request, the controller must provide that personal data to the individual in intelligible form.

4.2. Process for responding to access requests from individuals

4.2.1. If Twilio receives an access request from an individual, this must be passed to the Privacy Team at privacy@twilio.com immediately to make an initial assessment of responsibility consistent with the requirements of paragraph 3.2 above.

4.2.2. Where Twilio determines it is the controller of the personal data and responsible for responding to the individual directly (and that no exemption to the right of access applies under applicable data protection laws), the Privacy Team will arrange a search of all relevant electronic and paper filing systems.

4.2.3. The Privacy Team may refer any complex cases to the General Counsel / Chief Compliance Officer for advice, particularly where the request concerns information relating to third parties or where the release of personal data may prejudice commercial confidentiality or legal proceedings.

4.2.4. The personal data that must be disclosed to the individual will be collated by the Privacy Team into a readily understandable format. A covering letter will be prepared by the Privacy Team which includes all information required to be provided in response to an individual's access request (including the information described in paragraph 4.1.1).

4.3. Exemptions to the right of access

4.3.1. A valid request may be refused on the following grounds:

a. If the refusal to provide the information is consistent with applicable data protection law (for example, where a European Group Member transfers personal data under the Controller Policy, if the refusal to provide the information is consistent with the applicable data protection law in the European Member State where the Group Member is located);

b. where the personal data is held by Twilio in non-automated form that is not or will not become part of a filing system; or

c. the personal data does not originate from Europe, has not been processed by any European Group Member, and the provision of the personal data requires Twilio to use disproportionate effort.

d. The Privacy Team will assess each request individually to determine whether any of the above- mentioned exemptions applies. A Group Member must never apply an exemption unless this has been discussed and agreed with the Privacy Team.

5. Requests to correct, update or erase personal data, or to restrict or cease processing personal data

5.1. If Twilio receives a request to correct, update or erase personal data, or to restrict or cease processing of an individual's personal data, this must be passed to the Privacy Team at privacy@twilio.com immediately to make an initial assessment of responsibility consistent with the requirements of paragraph 3.2 above.

5.2. Once an initial assessment of responsibility has been made then:

a. where Twilio is the controller of that personal data, the request must be notified to the Privacy Team promptly for it to consider and deal with as appropriate in accordance with applicable data protection laws.

b. where a Customer is the controller of that personal data, the request must be notified to the Customer promptly for it to consider and deal with as appropriate in accordance with its duties under applicable data protection laws. Twilio shall assist the Customer to fulfil the request in accordance with the terms of its contract with the Customer.

5.3. To assist the Privacy Team in assessing an individual's request for restriction of processing of his or her personal data, the grounds upon which an individual may request restriction are when:

a. the accuracy of the personal data is contested by the individual, for a period enabling Twilio to verify the accuracy of the personal data;

b. the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of its use instead;

c. Twilio no longer needs the personal data for the purposes of the processing, but it is required by the individual for the establishment, exercise or defence of legal claims; or

d. Twilio has exercised his or her right to object pending the verification whether the legitimate grounds of the controller override his or her objection right.

5.4. To assist the Privacy Team in assessing an individual's request for erasure of his or her personal data, the grounds upon which an individual may request erasure are when:

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b. the individual withdraws consent on which the processing is based and there is no other legal ground for the processing;

c. the individual exercises its right to object to processing of his or her personal data and there are no overriding legitimate grounds for continued processing;

d. the personal data have been unlawfully processed;

e. the personal data have to be erased for compliance with a legal obligation to which the controller is subject; or

f. the personal data have been collected in relation to the offer of information society services to a child under the age of 16 and a parent or guardian has not consented to the processing.

5.5. When Twilio must rectify or erase personal data, either in its capacity as controller or on instruction of a Customer when it is acting as a processor, Twilio will notify other Group Members and any sub-processor to whom the personal data has been disclosed so that they can also update their records accordingly.

5.6. Where Twilio acting as a controller must restrict processing of an individual's personal data, it must inform the individual before it subsequently lifts any such restriction.

5.7. If Twilio acting as controller has made the personal data public, and is obliged to erase the personal data pursuant to a Data Protection Rights Request, it must take reasonable steps, including technical measures (taking account of available technology and the cost of implementation), to inform controllers which are processing the personal data that the individual has requested the erasure by such controllers of any links to, or copy or replication of, the personal data

6. Right to data portability

6.1. If an individual makes a Data Protection Rights Request to Twilio acting as controller to receive the personal data that he or she has provided to Twilio in a structured, commonly used and machine-readable format and/or to transmit directly such information to another controller (where technically feasible), Twilio's Privacy Team will consider and deal with the request appropriately in accordance with applicable data protection laws insofar as the processing is based on that individual's consent or on the performance of, or steps taken at the request of the individual prior to entry into, a contract.

7. Questions about this Data Protection Rights Procedure

7.1.1 All queries relating to this Procedure are to be addressed to the Privacy Team or at privacy@twilio.com.

Appendix 3

PRIVACY COMPLIANCE STRUCTURE

1. Introduction

1.1. Twilio's compliance with global data protection laws and the "Binding Corporate Rules: Controller Policy" and "Global Binding Corporate Rules: Processor Policy" (together the "Policies" or, respectively, the "Controller Policy" and the "Processor Policy") is overseen and managed throughout all levels of the business by a global, multi-layered, cross-functional privacy compliance structure.

1.2. Twilio's Privacy Compliance Structure has the full support of Twilio's executive management. Further information about Twilio's Privacy Compliance Structure is set out below and in the structure chart provided at Annex A.

2. General Counsel and Chief Compliance Officer

2.1. Twilio has appointed its General Counsel and Chief Compliance Officer ("GC/CCO") who provides executive-level oversight of, and has responsibility for, ensuring Twilio's compliance with applicable data protection laws and the Policies.

2.2. The GC/CCO reports directly to the Board of Directors on all material or strategic issues relating to Twilio's compliance with data protection laws and the Policies, and is also accountable to Twilio's independent Audit Committee. The GC/CCO leads and is supported by Twilio's Privacy Team.

2.3. The GC/CCO's key responsibilities with regard to privacy include:

- Ensuring that the Policies and other privacy-related policies, objectives and standards are defined and communicated.
- Reporting at least annually (and more often, if needed, in response to specific risks or concerns), on global data protection compliance to Twilio's Board of Directors.

- Providing clear and visible senior management support and resources for the Policies and for privacy objectives and initiatives in general.
- Evaluating, approving and prioritizing remedial actions consistent with the requirements of the Policies, strategic plans, business objectives and regulatory requirements.
- Periodically assessing privacy initiatives, accomplishments, and resources to ensure continued effectiveness and improvement.
- Ensuring that Twilio's business objectives align with the Policies and related privacy and information protection strategies, policies and practices.
- Facilitating communications on the Policies and privacy topics with the Board of Directors and independent Audit Committee.
- Dealing with any escalated privacy complaints in accordance with the Binding Corporate Rules: Complaint Handling Procedure.
- Supporting the conduct of any data protection audits carried out by data protection authorities, in accordance with the Binding Corporate Rules: Cooperation Procedure.

3. Privacy Team

3.1.1. The Twilio Privacy Team consists of Twilio's in-house privacy counsel, as well as other non-legal privacy operations staff, such as Twilio's Director of Privacy Operations. The Privacy Team reports directly to Twilio's Lead Privacy Counsel and Data Protection Officer, who in turn, reports to the GC/CCO. Reporting to the GC/CCO ensures appropriate independence and oversight of duties relating to all aspects of Twilio's data protection compliance.

3.2. The Privacy Team is accountable for managing and implementing Twilio's data privacy program internally (including the Policies) and for ensuring that effective data privacy controls are in place for any third party service provider Twilio engages. In this way, the Privacy Team is actively engaged in addressing matters relating to Twilio's privacy compliance on a routine, day-to-day basis.

3.3. The Privacy Team's responsibilities include:

- Providing guidance about the collection and use of personal data subject to the Policies and to assess the processing of personal data by Twilio Group Members for potential privacy-related risks.
- Responding to inquiries and compliance relating to the Policies from staff members, customers and other third parties raised through its dedicated e-mail address at privacy@twilio.com.
- Helping to implement the Policies and related policies and practices at a functional and local country level, providing guidance and responding to privacy questions and issues.
- Providing input on audits of the Policies, coordinating responses to audit findings and responding to inquiries of the data protection authorities.
- Monitoring changes to global privacy laws and ensuring that appropriate changes are made to the Policies and Twilio's related policies and business practices.

- Overseeing training for staff on the Policies and on data protection legal requirements in accordance with the Binding Corporate Rules: Privacy Training Program.
- Promoting the Policies and privacy awareness across business units and functional areas through privacy communications and initiatives.
- Evaluating privacy processes and procedures to ensure that they are sustainable and effective.
- Reporting periodically on the status of the Policies to the GC/CCO and Board of Directors and / or Audit Committee as appropriate.
- Ensuring that the commitments made by Twilio in relation to updating, and communicating updates to the Policies are met in accordance with the Binding Corporate Rules: Updating Procedure.
- Overseeing compliance with the Binding Corporate Rules: Data Protection Rights Procedure and the handling of any requests made under it.

4. Security Compliance and Assurance Team

4.1. Twilio's Security Compliance and Assurance team, which is made up of members of the wider Trust and Security Team, reports to the Chief Trust and Security Officer. This team has a number of specific responsibilities in relation to the implementation and oversight of the Policies and privacy matters more generally, including:

- Audit of attendance of privacy training courses as set out in the Binding Corporate Rules: Privacy Training Program.
- Overseeing independent audits of compliance with the Policies as set out in the Binding Corporate Rules: Audit Protocol and ensuring that such audits address all aspects of the Policies.
- Ensuring that any issues or instances of non-compliance with the Policies are brought to the attention of Twilio's Privacy Team and that any corrective actions are determined and implemented within a reasonable time.

5. Privacy Committee

5.1.Twilio's Privacy Committee comprises functional leads or key representatives from the main functional areas within Twilio, including sales, marketing, HR, procurement, product development, legal and compliance.

5.2. The key responsibilities of Members of the Privacy Committee include:

- Promoting the Policies at all levels in their functional areas.
- Assisting the Privacy Team with the day-to-day implementation and enforcement of Twilio's privacy policies (including the Policies) within their respective areas of responsibility.
- Escalating questions and compliance issues or communicate any actual or potential violation of relating to the Policies to the Privacy Team.

- Through its liaison with the Privacy Team, the Privacy Committee serves as a channel through which the Privacy Team can communicate data privacy compliance actions to all key functional areas of the business.

5.3. The Privacy Committee will meet on a formal and regular basis, at a minimum frequency of every six months, to ensure a coordinated approach to data protection compliance across all functions.

6. Twilio Staff

6.1. All staff members within Twilio are responsible for supporting the functional Privacy Committee members on a day-to-day basis and adhering to Twilio privacy policies.

6.2. In addition, Twilio personnel are responsible for escalating and communicating any potential violation of the privacy policies to the appropriate Privacy Committee member or, if they prefer, the Twilio Privacy Team. On receipt of a notification of a potential violation of the privacy policy the issue will be investigated to determine if an actual violation occurred. Results of such investigations will be documented.

Appendix 4

PRIVACY TRAINING PROGRAM

1. Background

1.1. The “Binding Corporate Rules: Controller Policy” and “Binding Corporate Rules: Processor Policy” (together the “Policies” or, respectively, the "Controller Policy"and the "Processor Policy") provide a framework for the transfer of personal data between Twilio's group members ("Group Members"). The document sets out the requirements for Twilio to train its staff members on the requirements of the Policies.

1.2. Twilio must train staff members (including new hires, temporary staff and individual contractors whose roles bring them into contact with personal data) on the basic principles of data protection, confidentiality and information security awareness. This must include training on applicable data protection laws, including European data protection laws. Training shall also include guidance on data protection best practices and any security certifications applicable to Twilio such as ISO 27001. This training is repeated on a regular basis.

1.3. Staff members who have permanent or regular access to personal data and who are involved in the processing of personal data or in the development of tools to process personal data must receive additional, tailored training on the Policies and specific data protection issues relevant to their role.

1.4. These trainings are further described below.

2. Responsibility for the Privacy Training Program

2.1. Twilio's Privacy Team has overall responsibility for privacy training at Twilio, with input from colleagues from other functional areas, including Legal, Information Security, Security Compliance and Assurance, HR and other departments, as appropriate. The Privacy Team will review training from time to time to ensure it addresses all relevant aspects of the Policies and that it is appropriate for individuals who have permanent or regular access to personal data, who are involved in the processing of personal data or in the development of tools to process personal data.

2.2. Twilio's senior management is committed to the delivery of data protection training courses, and will ensure that staff are required to participate, and given appropriate time to attend, such courses. Course attendance must be recorded and monitored via regular audits of the training process. These audits are performed by Twilio's Security Compliance and Assurance Team and/or independent third party auditors.

1. If these training audits reveal persistent non-attendance, this will be escalated to the Privacy Team for action. Such action may include escalation of non-attendance to appropriate managers within Twilio who will be responsible and held accountable for ensuring that the individual(s) concerned attend and actively participate in such training.

3. Delivery of the training courses

3.1. Twilio will deliver mandatory training courses, either in person or electronically, supplemented by face to face training for staff members. The courses are designed to be both informative and user-friendly, generating interest in the topics covered.

3.2. All Twilio staff members must complete data protection training (including training on the Policies):

a. as part of their induction program;

b. as part of a regular refresher training at least every year;

c. as and when necessary to stay aware of changes in the law; and

d. as and when necessary to address any compliance issues arising from time to time.

3.3. Certain staff members must receive supplemental specialist training, in particular staff members who handle customer or employee personal data in Product Development, HR and Customer Support or whose business activities include processing special categories of personal data. Specialist training shall be delivered as additional modules to the basic training package, and will be tailored as necessary to the course participants.

4. Training on data protection

4.1. Twilio's training on data protection and the Policies will cover the following main areas:

4.1.1. Background and rationale:

a. What is data protection law?

b. What are key data protection terminology and concepts?

c. What are the data protection principles?

d. How does data protection law affect Twilio internationally?

e. What are Twilio's BCR Policies?

4.1.2. The Policies:

a. An explanation of the Policies

b. The scope of the Policies

c. The requirements of the Policies

d. Practical examples of how and when the Policies apply

e. The rights that the Policies give to individuals

f. The privacy implications arising from processing personal data for clients

4.1.3. Where relevant to a staff member's role, training will cover the following procedures under the Policies:

a. Data Subject Rights Procedure

b. Audit Protocol

c. Updating Procedure

d. Cooperation Procedure

e. Complaint Handling Procedure

f. Government Data Request Procedure

Appendix 5

AUDIT PROTOCOL

Binding Corporate Rules: Audit Protocol

1. Background

1.1. Twilio's “Binding Corporate Rules: Controller Policy” and “Binding Corporate Rules: Processor Policy” (together the “Policies” or, respectively, the "Controller Policy"and the "Processor Policy") safeguard personal data transferred between the Twilio group members ("Group Members").

1.2. Twilio must audit its compliance with the Policies on a regular basis, and this document describes how and when Twilio must perform such audits. Although this Audit Protocol describes the formal assessment process by which Twilio will audit its compliance with the Policies, this is only one way in which Twilio ensures that the provisions of the Policies are observed and corrective actions taken as required.

1.3. In particular, Twilio's Privacy Tteam provides ongoing guidance about the processing of personal data and continually assesses the processing of personal data by Group Members for potential privacy-related risks and compliance with these Policies.

2. Conduct of an audit

Overview of audit requirements

2.1. Compliance with the Policies is overseen on a day to day basis by the Security Compliance and Assurance Team. The Security Compliance and Assurance Team is responsible for overseeing independent audits of compliance with the Policies and will ensure that such audits address all aspects of the Policies.

2.2. The Security Compliance and Assurance Team is responsible for ensuring that any issues or instances of non-compliance with the Policies are brought to the attention of the Privacy Team and that any corrective actions are determined and implemented within a reasonable time. Serious non-compliance issues will be escalated to General Counsel and Chief Compliance Officer and, ultimately, the Board of Directors in accordance with paragraph 2.10.

2.3. Where Twilio acts as a processor, the Customer (or auditors acting on its behalf) may audit Twilio for compliance with the commitments made in the Processor Policy and may extend such audits to any sub-processors acting on Twilio's behalf in respect of such processing. Such audits shall be conducted in accordance with the terms of Customer's contract with Twilio.

Frequency of audit

2.4. Audits of compliance with the Policies are conducted:

a. at least annually in accordance with Twilio's audit procedures; and/or

b. at the request of the General Counsel and Chief Compliance Officer and / or the Board of Directors; and/or

c. as determined necessary by the Privacy Team or Audit Committee (for example, in response to a specific incident) and / or

d. (with respect to audits of the Processor Policy), as required by the terms of the Customer's contract with Twilio.

Scope of audit

2.5. The Privacy Team will determine the scope of an audit following a risk-based analysis that takes into account relevant criteria such as:

a. areas of current regulatory focus;

b. areas of specific or new risk for the business;

c. areas with changes to the systems or processes used to safeguard data;

d. use of innovative new tools, systems or technologies;

e. areas where there have been previous audit findings or complaints;

f. the period since the last review; and

g.the nature and location of the personal data processed.

2.6. In the event that a Customer exercises its right to audit Twilio for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, data files and documentation relating to that Customer. Twilio will not provide a Customer with access to systems which process personal data of another Customer.

Auditors

2.7. Audit of the Policies (including any related procedures and controls) will be undertaken by independent and experienced professional auditors appointed by Twilio and acting under a duty of confidence and in possession of the required professional qualifications as necessary to perform audits of the Policies.

2.8. In the event that a Customer exercises its right to audit Twilio for compliance with the Processor Policy, such audit may be undertaken by that Customer, or by independent and suitably experienced auditors approved by that Customer, in accordance with the terms of the Customer's contract with Twilio.

2.9. The competent data protection authorities may audit Group Members for the purpose of reviewing compliance with the Policies (including any related procedures and controls) in accordance with the Binding Corporate Rules: Cooperation Procedure.

Reporting

2.10. Data protection audit reports must be submitted to the General Counsel and Chief Compliance Officer, Lead Privacy Counsel and Data Protection Officer, and the Chief Trust and Security Officer, and, if the report reveals breaches or the potential for breaches of a serious nature (for example, presenting a risk of potential harm to individuals or to the business), to the Board of Directors.

2.11. Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Twilio will:

a. provide copies of the results of data privacy audits of the Policies (including any related procedures and controls) to competent data protection authorities; and

b. to the extent that an audit of compliance with the Processor Policy relates to personal data Twilio processes on behalf of a Customer, to that Customer.

2.12. The Lead Privacy Counsel and Data Protection Officer is responsible for liaising with the competent data protection authorities for the purpose of providing the information outlined in paragraph 2.11.

Appendix 6

COMPLAINT HANDLING PROCEDURE

1. Background

Twilio's "Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the “Policies” or, respectively, the "Controller Policy"and the "Processor Policy") safeguard personal data transferred between the Twilio group members ("Group Members").

This Complaint Handling Procedure describes how complaints brought by an individual whose personal data is processed by Twilio under the Policies must be addressed and resolved.

This procedure will be made available to individuals whose personal data is processed by Twilio under the Controller Policy and to Customers on whose behalf Twilio processes personal data under the Processor Policy.

2. How individuals can bring complaints

Any individuals may raise a data protection question, concern or complaint (whether related to the Policies or not) by e-mailing Twilio’s Privacy Team at privacy@twilio.com or by writing to Twilio’s Privacy Team at 375 Beale Street, Suite 300, San Francisco, CA 94105.

3. Complaints where Twilio is a controller

Who handles complaints?

3.1.1. The Privacy Team will handle all questions, concerns, or complaints in respect of personal data for which Twilio is a controller (such as personal data processed in the context of human resources administration or customer relationship management), including questions, concerns or complaints arising under the Controller Policy. The Privacy Team will liaise with colleagues from relevant business and support units as necessary to address and resolve such questions, concerns and complaints.

What is the response time?

3.1.2. Twilio will acknowledge receipt of a question, concern or complaint to the individual concerned without undue delay, investigating and making a substantive response within one (1) month.

3.1.3. If, due to the complexity of the complaint, a substantive response cannot be given within this period, Twilio will advise the individual accordingly and provide a reasonable estimate (not exceeding three (3) months in total) of the timescale within which a substantive response will be provided.

What happens if an individual disputes a finding?

3.1.4. If the individual notifies Twilio that it disputes any aspect of the response finding, the Privacy Team will refer the matter to the General Counsel and Chief Compliance Officer (GC/CCO). The GC/CCO will review the case and advise the individual of his or her decision either to accept the original finding or to substitute a new finding. The GC/CCO will respond to the complainant within one (1) month from being notified of the escalation of the dispute.

3.1.5. As part of its review, the GC/CCO may arrange to meet the parties to the dispute in an attempt to resolve it. If, due to the complexity of the dispute, a substantive response cannot be given within one (1) month of its escalation, the GC/CCO will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided which will not exceed three (3) months from the date the dispute was escalated.

3.1.6. If the complaint is upheld, the GC/CCO will arrange for any necessary steps to be taken as a consequence.

4. Complaints where Twilio is a processor

Communicating complaints to the Customer

4.1.1. Where a complaint is brought in respect of the processing of personal data for which Twilio is a processor on behalf of a Customer, Twilio will communicate the details of the complaint to the relevant Customer without delay and without handling it (unless Twilio has agreed in the terms of its contract with the Customer to handle complaints).

4.1.2. Twilio will cooperate with the Customer to investigate the complaint, in accordance with the terms of its contract with the Customer and if so instructed by the Customer.

What happens if a Customer no longer exists?

4.1.3. In circumstances where a Customer has disappeared, no longer exists or has become insolvent, and no successor entity has taken its place, individuals whose personal data are processed under the Processor Policy have the right to complain to Twilio and Twilio will handle such complaints in accordance with paragraph 3 of this Complaint Handling Procedure.

4.1.4. In such cases, individuals also have the right to complain to a competent data protection authority and to file a claim with a court of competent jurisdiction, including where they are not satisfied with the way in which their complaint has been resolved by Twilio. Such complaints and proceedings will be handled in accordance with paragraph 5 of this Complaint Handling Procedure.

5. Right to complain to a competent data protection authority and to commence proceedings

Overview

5.1.1 Where individuals' personal data:

a. are processed in Europe by a Group Member acting as a controller and/or transferred to a Group Member located outside Europe under the Controller Policy; or

b. are processed in Europe by a Group Member acting as a processor and/or transferred to a Group Member located outside Europe under the Processor Policy;

then those individuals have certain additional rights to pursue effective remedies for their complaints, as described below.

5.1.2 The individuals described in above have the right to complain to a competent data protection authority (in accordance with paragraph 5.2) and/or to commence proceedings in a court of competent jurisdiction (in accordance with paragraph 5.3), whether or not they have first complained directly to the Customer in question or to Twilio.

5.1.3. Twilio accepts that complaints and claims made pursuant to paragraphs 5.2 and 5.3 may be lodged by a not-for-profit body, organization or association acting on behalf of the individuals concerned.

5.2. Complaint to a data protection authority

5.2.1. If such an individual wishes to complain about Twilio's processing of his or her personal data to a data protection authority on the basis that a European Group Member has processed personal data in breach of the Policies or in breach of applicable data protection laws, he or she may complain about that European Group Member to the data protection authority in the European territory:

a. of his or her habitual residence;
b. of his or her place of work; or
c. where the alleged infringement occurred.

5.2.2.
If an individual wishes to complain about Twilio's processing of his or her personal data to a data protection authority on the basis that a non-European Group Member has processed personal data in breach of the Policies or in breach of applicable data protection laws, then Twilio Ireland Limited will submit to the jurisdiction of the competent data protection authority (determined in accordance with paragraph 5.2.1 above) in place of that non-European Group Member, as if the alleged breach had been caused by Twilio Ireland Limited.

5.3. Proceedings before a national court

5.3.1. If an individual wishes to commence court proceedings against Twilio on the basis that a European Group Member has processed personal data in breach of the Policies or in breach of applicable data protection 12 laws, then he or she may commence proceedings against that European Group Member in the European territory:
a. In which that European Group Member is established; or
b. of his or her habitual residence.

5.3.2.
If an individual wishes to commence court proceedings against Twilio on the basis that a non-European Group Member has processed personal data in breach of the Policies or in breach of applicable data protection laws, then Twilio Ireland Limited will submit to the jurisdiction of the competent data court (determined in accordance with paragraph 5.3.1 above) in place of that non-European Group Member, as if the alleged breach had been caused by Twilio Ireland Limited.

Appendix 7

CO-OPERATION PROCEDURE

1. Introduction

1.1. This Binding Corporate Rules: Cooperation Procedure sets out the way in which Twilio will cooperate with competent data protection authorities in relation to the "Twilio Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the “Policies” or, respectively, the "Controller Policy"and the "Processor Policy").

2. Cooperation Procedure

2.1. Where required, Twilio will make the necessary personnel available for dialogue with a competent data protection authority in relation to the Policies.

2.2. Twilio will review, consider and (as appropriate) implement:

a. any advice or decisions of relevant competent data protection authorities on any data protection law issues that may affect the Policies; and

b. any guidance published by data protection authorities (including the European Data Protection Board or any successor to it) in connection with Binding Corporate Rules for Processors and Binding Corporate Rules for Controllers.

2.3. Subject to applicable data protection law and respect for the confidentiality and trade secrets of the information provided, Twilio will provide upon request copies of the results of any audit it conducts of the Policies to a competent data protection authority.

2.4. Twilio agrees that:

a. a competent data protection authority may audit any Group Member located within its jurisdiction for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction; and

b. a competent data protection authority may audit any Group Member who processes personal data for a Customer established within the jurisdiction of that data protection authority for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction;

2.5. and with full respect to the confidentiality of the information obtained and to the trade secrets of Twilio (unless this requirement is in conflict with applicable data protection law).

2.6. Twilio agrees to abide by a formal decision of any competent data protection authority on any issues relating to the interpretation and application of the Policies (unless and to the extent that Twilio is entitled to appeal any such decision and has chosen to exercise such right of appeal).

Appendix 8

UPDATING PROCEDURE

1. Introduction

1.1. This Binding Corporate Rules: Updating Procedure describes how Twilio must communicate changes to the "Binding Corporate Rules: Controller Policy" ("Controller Policy") and to the "Binding Corporate Rules: Processor Policy" ("Processor Policy") (together the "Policies") to competent data protection authorities, individual data subjects, its Customers and to Twilio group members ("Group Members") bound by the Policies.

1.2. Any reference to Twilio in this procedure is to the Privacy Team who is accountable for ensuring that the commitments made by Twilio in this Updating Procedure are met.

2. Records keeping

2.1. Twilio must maintain a change log which sets out details of each and every revision made to the Policies, including the nature of the revision, the reasons for making the revision, the date the revision was made, and who authorised the revision.

2.2. Twilio must also maintain an accurate and up-to-date list of Group Members that are bound by the Policies and of the sub-processors appointed by Twilio to process personal data on behalf of Customers. This information will be made available online or provided upon request from Twilio to competent data protection authorities and to Customers and individuals who benefit from the Policies.

2.3. The Data Compliance team shall be responsible for ensuring that the records described in this paragraph 2 are maintained and kept accurate and up-to-date.

3. Changes to the Policies

3.1. All proposed changes to the Policies must be reviewed and approved by the Lead Privacy Counsel in order to ensure that a high standard of protection is maintained for the data protection rights of individuals who benefit from the Policies. No changes to the Policies shall take effect unless reviewed and approved by the Lead Privacy Counsel.

3.2. Twilio will communicate all changes to the Policies (including reasons that justify the changes) and changes to the list of Group Members bound by the Policies:

a. to the Group Members bound by the Policies via written notice (which may include e-mail);

b. systematically to Customers and the individuals who benefit from the Policies via www.twilio.com (https://www.twilio.com/) (and, if any changes materially affect Twilio's processing operations on behalf of a Customer, they must be communicated to Customers before they take effect, in accordance with paragraph 4.2 below); and

c. to the data protection authority that was the lead authority for the purposes of granting Twilio's BCR authorisation ("Lead Authority"), and any other relevant data protection authorities the Lead Authority may direct, at least once a year. authorities upon request.

4. Communication of substantial changes

4.1. If Twilio makes any substantial changes to the Policies or to the list of Group Members bound by the Policies, that would affect the level of protection offered by the Policies, or otherwise significantly affect the Policies (for example, by making changes to the binding nature of the Policies), it will promptly report such changes to the Lead Authority.:

a. the Data Protection Authority that was the lead authority for the purposes of granting Twilio's BCR authorisation (the "Lead Authority"); and

b. to any other relevant data protection authorities as may either be directed by the Lead Authority or as the Privacy Team considers necessary taking into account Twilio's obligations under applicable data protection laws and guidance from the data protection authorities.

4.2. If a proposed change to the Processor Policy will materially affect Twilio's processing of personal data on behalf of a Customer, Twilio will also:

a. actively communicate the proposed change to the affected Customer before it takes effect, and with sufficient notice to enable the affected Customer to raise objections; and

b. the Customer may then suspend the transfer of personal data to Twilio and/or terminate the contract in accordance with the terms of its contract with Twilio.

5. Transfers to new Group Members

5.1. If Twilio intends to transfer personal data to any new Group Members under the Policies, it must first ensure that all such new Group Members are bound by the Policies before transferring personal data to them.

Appendix 9

Government Data Request Procedure

1. Introduction

1.1. This Binding Corporate Rules: Government Data Request Procedure sets out Twilio's procedure for responding to a request received from a law enforcement or state security body (together the "Requesting Authority") to disclose personal data processed by Twilio (hereafter "Data Disclosure Request").

1.2. Where Twilio receives a Data Disclosure Request, it will handle that Data Disclosure Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal data than is required by this Procedure, Twilio will comply with the relevant requirements of applicable data protection law(s).

2. General principle on Data Disclosure Requests

2.1. As a general principle, Twilio does not disclose personal data in response to a Data Disclosure Request unless either:
a. it is under a compelling legal obligation to make such disclosure; or
b. taking into account the nature, context, purposes, scope and urgency of the Data Disclosure Request and the privacy rights and freedoms of any affected individuals, there is an imminent risk of serious harm that merits compliance with the Data Disclosure Requests in any event.

2.2. For that reason, unless it is legally prohibited from doing so or there is an imminent risk of serious harm, Twilio will notify and cooperate with the competent data protection authorities and, where it processes the requested personal data on behalf of a Customer, the Customer, in order to address the Data Disclosure Request. Even where disclosure is required, Twilio's policy is that the Customer should have the opportunity to protect the personal data requested because it has the greatest interest in opposing, or is in the better position to comply with, a Data Disclosure Request.

3. Handling of a Data Disclosure Request

3.1. Receipt of a Data Disclosure Request

3.1.1. If a Twilio Group Member receives a Data Disclosure Request, the recipient of the request must pass it to Twilio's Legal Requests team immediately upon receipt, indicating the date on which it was received together with any other information that may assist Twilio's Legal Requests team to deal with the request.

3.1.2. The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Disclosure Request. Any Data Disclosure Request, howsoever made, must be notified to the Legal Requests Team for review.

3.2. Initial Steps

3.2.1. Twilio's Legal Requests team will carefully review each and every Data Disclosure Request on a case-by-case basis. Twilio's Legal Requests team will liaise with others within the legal department and outside counsel as appropriate to deal with the request to determine the nature, context, purposes, scope and urgency of the Data Disclosure Request, as well as its validity under applicable laws, in order to identify whether action may be needed to challenge the Data Disclosure Request.

4. Notice of a Data Disclosure Request

4.1. Notice to the EEA Customer

4.1.1. Where Twilio is processing personal data on behalf of an EEA Customer, after assessing the nature, context, purposes, scope and urgency of the Data Protection Request, Twilio will notify and provide the EEA Customer with the details of the Data Disclosure Request prior to disclosing any personal data, unless

legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

4.2. Notice to the competent Data Protection Authorities

4.2.1. Twilio will also put the request on hold in order to notify and consult with the competent Data Protection Authorities, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

4.2.2. Where Twilio is prohibited from notifying the competent Data Protection Authorities and suspending the request, Twilio will use its best efforts (taking into account the nature, context, purposes, scope and urgency of the request) to inform the Requesting Authority about its obligations under applicable data protection law and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that Twilio can consult with the competent Data Protection Authorities, which may also, in appropriate circumstances, include seeking a court orde to this effect. Twilio will maintain a written record of the efforts it takes.

5. Transparency Reports

5.1. If, despite having used its best efforts, Twilio is not in a position to notify the competent Data Protection Authorities of the request, Twilio commits to preparing an annual report (a "Transparency Report") which reflects to the extent permitted by applicable laws, the number and type of Data Disclosure Requests it has received in the preceding year and, if possible, the Requesting Authorities who made those requests. Twilio shall provide this report to the lead data protection authority which authorized its BCR (and any other data protection authorities that the lead authority may direct) once a year.

6. Bulk transfers

6.1. In no event will any Group Member transfer personal data to a Requesting Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

Appendix 10

EXCLUDED PRODUCTS

- SendGrid branded services
- Teravoz branded services