Twilio Acceptable Use Policy

Effective Date: March 18, 2020

This Acceptable Use Policy ("*AUP*") applies to Customer's use of the Services offered by Twilio Inc. or any of its Affiliates. In the event of any conflict or inconsistency among the following documents, and, except as otherwise set expressly forth in an Order Form, the order of precedence shall be (1) this AUP, (2) product-specific terms, (3) the Agreement, and (4) the Documentation.

Note: The SendGrid E-Mail Policy is replaced in its entirety by this AUP, made effective as of January 1, 2020, including updates made from time to time to this AUP.

Definitions

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

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

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

"*Sensitive Data*" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), financial information, banking account numbers or passwords; (c)

employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords, mother's maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of "special categories of data" under GDPR or any other applicable law relating to privacy and data protection.

Capitalized terms in this AUP that are not otherwise defined in this AUP have the meanings given in the Agreement.

Prohibited Uses

Customer agrees not to use, and, not to encourage or allow any End User to use, the Services in the following prohibited ways:

1. Using the Services in a manner that is or otherwise encourages (a) any illegal, fraudulent, or abusive activities or (b) materially interfering with the business or activities of Twilio or harms other Twilio customers.
2. Attempting to bypass or break any security mechanism on any of the Services or using the Services in any other manner that poses a material security or service risk to Twilio or any of its other customers.
3. Reverse-engineering the Services in order to find limitations, vulnerabilities, or evade filtering capabilities.
4. Launching or facilitating, whether intentionally or unintentionally, a denial of service attack on any of the Services or any other conduct that materially and adversely impacts the availability, reliability, or stability of the Services.
5. Transmitting any material, data, or content that contains viruses, Trojan horses, spyware, worms or any other malicious, harmful, or deleterious programs.
6. Violating or facilitating the violation of any applicable laws or regulations of any applicable jurisdiction, including, without limitation, (a) applicable laws or regulations related to the transmission of data and recording or monitoring of phone calls and other forms of communication; (b) applicable laws or regulations that prohibit engaging in any unsolicited advertising, marketing, or transmission of communications; (c) applicable anti-spam laws or regulations such as the CAN SPAM Act of 2003, the Telephone Consumer Protection Act, and the Do-Not-Call Implementation Act; or (d) applicable data protection or privacy laws, regulations, or legislation.
7. Using the Services in connection with unsolicited, unwanted, or harassing communications (commercial or otherwise), including, but not limited to, phone calls, SMS or MMS messages, chat, voice mail, video, email, or faxes.

8. Using the Services to harvest or otherwise collect information about individuals, including email addresses or phone numbers, without their explicit consent or under false pretenses.
9. Using the Services to receive, send or otherwise process Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 as amended, unless Customer has signed a Business Associate Agreement with Twilio or Customer's use of the Services fits within the "conduit" or some other exception for requiring a Business Associate Agreement.
10. Using the Twilio Services to record or monitor a phone call or other communication without securing consent from the participants to the phone call or other communication as required under applicable law (including, as applicable, California's Invasion of Privacy Act and similar laws in other jurisdictions).
11. Using the Services in a manner that generates inquiries from a law enforcement, government, or regulatory agency or triggers such an agency to request the suspension of the Services to Customer and/or Customer's phone numbers.
12. Using the Services to transmit any material, data, or content that infringes the intellectual property rights or other rights of third parties.
13. Using the Services to transmit any material or content that is, facilitates, or encourages libelous, defamatory, discriminatory, or otherwise malicious or harmful speech or acts to any person or entity, including but not limited to hate speech, and any other material or content that Twilio reasonably believes degrades, intimidates, incites violence against, or encourages prejudicial action against anyone based on age, gender, race, ethnicity, national origin, religion, sexual orientation, disability, geographic location or other protected category.
14. Creating a false identity or forged email address or header, or phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message, email, or phone call.
15. Using the Twilio Services in any manner that causes a telecommunications provider to complain about such use to Twilio or materially violates the following: (a) industry standards, policies and applicable guidelines published by (i) the CTIA (Cellular Telecommunications Industry Association), (ii) the Mobile Marketing Association, or (iii) any other generally recognized industry associations; (b) telecommunications provider guidelines and usage requirements as communicated in writing by Twilio to Customer.
16. Using the Twilio Services in a manner that violates the Twilio Messaging Policy available at http://www.twilio.com/legal/messaging-policy (http://www.twilio.com/legal/messaging-policy).
17. Using the Twilio Services to transmit any material or content that is offensive, inappropriate, pornographic, obscene, illegal, or otherwise objectionable to any person or entity, including cannabis-related terms or images.

18. Using or attempting to use the Twilio Services to contact or allow End Users to contact Emergency Services, unless certain Twilio Services are expressly approved for Emergency Services and Customer strictly uses those Twilio Services in accordance with the Emergency Services Addendum available at http://www.twilio.com/legal/tos (http://www.twilio.com/legal/tos). The Twilio Services that are expressly approved for Emergency Services are also identified at http://www.twilio.com/legal/tos (http://www.twilio.com/legal/tos).

19. Having, in a given month, (a) a high volume of unanswered outbound phone calls, (b) a low average outbound call duration (i.e., outbound phone calls, on average, that are generally less than twelve (12) seconds in length), or (c) outbound phone calls that are too short in duration (i.e., outbound phone calls generally less than twelve (12) seconds in length). Twillio will cooperate In trace back investigations by identifying the upstream provider from which the suspected illegal robocall entered Twilio's network or by identifying its own customer if the call originated in Twilio's network.

20. Using the SendGrid Services in a way that violates generally recognized industry guidelines, including, without limitation, (a) using non-permission based email lists (i.e., lists in which each recipient has not explicitly granted permission to receive emails from Customer by affirmatively opting-in to receive those emails); (b) using purchased or rented email lists; (c) using third party email addresses, domain names, or mail servers without proper permission; (d) sending emails to non-specific addresses (e.g., webmaster@domain.com or info@domain.com); (e) sending emails that result in an unacceptable number of spam or unsolicited commercial email complaints (even if the emails themselves are not actually spam or unsolicited commercial email); (f) failing to include a working "unsubscribe" link in each email that allows the recipient to remove themselves from Customer's mailing list; (g) failing to comply with any request from a recipient to be removed from Customer's mailing list within 10 days of receipt of the request; (h) failing to include in each email a link to the then-current privacy policy applicable to that email; (i) disguising the origin or subject matter of any email or falsifying or manipulating the originating email address, subject line, headers, or transmission path information for any email; (j) failing to include in each email Customer's valid physical mailing address or a link to that information; and (k) including "junk mail," "chain letters," "pyramid schemes," incentives (e.g., coupons, discounts, awards, or other incentives) or other material in any email that encourages a recipient to forward the email to another recipient.

General Acceptable Use Guidelines

Phone Number Reclamation. Customer acknowledges that all phone numbers used in connection with the Twilio Services are subject to rules and restrictions imposed by telecommunications providers. In order to comply with such rules and restrictions, Twilio may, at its sole discretion, reclaim Customer's phone numbers that do not have adequate usage, as determined by such telecommunications providers. Twilio, however, will use commercially reasonable efforts to (a) provide notice to Customer prior to any phone

number reclamation and (b) to work with telecommunications providers to prevent the reclamation of any phone numbers. As a general rule of thumb, Twilio recommends that Customer regularly uses its phone numbers.

Separately, Twilio may reclaim, without prior notice, (a) any phone numbers associated with a trial Twilio account that have not been used for more than thirty (30) days or (b) any phone numbers associated with a Twilio account that has been suspended for more than thirty (30) days.

Sensitive Data. Customer acknowledges that the Services are not intended for the processing of Sensitive Data. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing any Sensitive Data over the Services, or prior to permitting End Users to transmit or process Sensitive Data over the Services. Except in the context of a specific agreement between the parties regarding the processing of Sensitive Data, any transmission or processing of Sensitive Data is solely at Customer's own risk. Twilio will have no additional liability, including, without limitation, any indemnification obligations, whatsoever in connection with any Sensitive Data transmitted or processed via the Services.

Updates to this AUP

Prior Notice: Twilio may update the terms of this AUP from time to time by providing Customer with prior written notice of material updates at least thirty (30) days in advance of the effective date. Notice will be given in Customer's account portal or via an email to the email address owner of Customer's account. This notice will highlight the intended updates. Except as otherwise specified by Twilio, updates will be effective upon the date indicated at the top of this AUP. The updated version of the AUP will supersede all prior versions.

Your Acceptance: Following such notice, Customer's continued access or use of the Services on or after the effective date of the changes to the AUP constitutes Customer's acceptance of any updates. If Customer does not agree to any updates, Customer should stop using the Services.

Exceptions: Twilio may not be able to provide at least thirty (30) days prior written notice of updates to this AUP that result from changes required by law or requirements from telecommunications providers.