Print this page

- Customer and Partner Agreements
- Privacy
- Mobile Application Terms
- Supplier Agreements
- Intellectual Property
- Resources for Law Enforcement
- Civil Requests
- Code of Conduct & Ethics Hotline
- Digital Promotions General Rules
- Customer Research and User Experience
- Legal Notices for Twilio's Web Site
- Italy ALIAS Database Code of Conduct

Twilio Acceptable Use Policy

Last Updated: February 25, 2025

This Acceptable Use Policy ("***AUP***") describes rules that apply to any party ("***you***", "***your***", "***yours***", or "***Customer***") using any products and services provided by Twilio Inc. or any of its affiliates ("***Services***") and any user of the Services, including via any products and services provided by Customer ("***End User***"). Twilio Inc. together with its affiliates will be referred to as "***Twilio***" in this AUP. The prohibited conduct in this AUP is not exhaustive. Customer is responsible for its End Users' compliance with this AUP and making its End Users aware of this AUP. If Customer or any End User violates this AUP, Twilio may suspend Customer's use of the Services. This AUP may be updated by Twilio from time to time upon reasonable notice, which may be provided via Customer's account, e-mail, or by posting an updated version of this AUP at https://www.twilio.com/legal/aup.

No Inappropriate Content or Users. Do not use the Services to transmit or store any content or communications (commercial or otherwise) that is illegal, harmful, unwanted, inappropriate, or objectionable, including, but not limited to, content or communications which Twilio determines (a) is false or inaccurate; (b) is hateful or encourages hatred or violence against individuals or groups; or (c) could endanger public safety. This prohibition includes use of the Services by a hate group. Customer and its End Users are also prohibited from using the Services to promote, or enable the transmission of or access to, any prohibited content or communications described in this paragraph.

Prohibited Activities. Do not use the Services to engage in or encourage any activity that is illegal, deceptive, harmful, a violation of others' rights, or harmful to Twilio's business operations or reputation, including:

- **Violations of Laws or Standards.** Violating laws, regulations, governmental orders, industry standards, or telecommunications providers' requirements or guidance in any applicable jurisdiction, including any of the foregoing that require (a) consent be obtained prior to transmitting, recording, collecting, or monitoring data or communications or (b) compliance with opt-out requests for any data or communications.
- **Interference with the Services.** Interfering with or otherwise negatively impacting any aspect of the Services or any third-party networks that are linked to the Services.
- **Reverse Engineering.** Reverse engineering, copying, disassembling, or decompiling the Services.
- **Falsification of Identity or Origin.** Creating a false identity or any attempt to mislead others as to the identity of the sender or the origin of any data or communications.

No Service Integrity Violations. Do not violate the integrity of the Services, including:

- **Bypassing Service Limitations.** Attempting to bypass, exploit, defeat, or disable limitations or restrictions placed on the Services.
- **Security Vulnerabilities.** Finding security vulnerabilities to exploit the Services or attempting to bypass any security mechanism or filtering capabilities.
- **Disabling the Services.** Any denial of service (DoS) attack on the Services or any other conduct that attempts to disrupt, disable, or overload the Services.
- **Harmful Code or Bots.** Transmitting code, files, scripts, agents, or programs intended to do harm, including viruses or malware, or using automated means, such as bots, to gain access to or use the Services.
- **Unauthorized Access.** Attempting to gain unauthorized access to the Services.

Data Safeguards. Customer is responsible for determining whether the Services offer appropriate safeguards for Customer's use of the Services, including, but not limited to, any safeguards required by applicable law or regulation, prior to transmitting or processing, or prior to permitting End Users to transmit or process, any data or communications via the Services.

Service and Country Specific Requirements. Additional requirements for specific (a) Services, including any country specific requirements, and (b) products and services that are purchased from Twilio, but provided, or otherwise made available, by a third party are, in either case, set forth at https://www.twilio.com/legal/service-country-specific-terms and apply solely to the extent Customer uses those specific (i) Services or (ii) third-party products and services.

Violations of this AUP, including any prohibited content or communications, may be reported to https://www.twilio.com/help/abuse. Customer agrees to immediately report any violation of this AUP to Twilio and provide cooperation, as requested by Twilio, to investigate and/or remedy that violation.