



Act-On Software, Inc.

Act-On Acceptable Use Policy

Effective: April 25, 2023

This Acceptable Use Policy (“AUP”) establishes certain rules and requirements pertaining to the use of Act-On Software, Inc.’s (“Act-On”) websites, products or services (collectively the “Services”). This AUP may be amended at any time and such amendment or termination will be effective at the time Act-On posts the revised AUP to its website(s). This AUP is incorporated by reference into the definitive agreement between Act-On and the Customer regarding such Services (“Agreement”). Capitalized terms not defined in this AUP will have the meanings set forth in the Agreement.

1. Compliance

This AUP is intended to protect the Customers, Partners (as defined below), and individual users of Act-On’s Services (such Customers, Partners and users singularly and collectively referred to as “Users”) and the Internet community as a whole from improper, inappropriate, abusive, or illegal activity. When using any Act-On Services, all Users, including but not limited to any end Users of the Services sublicensed, resold or otherwise made available to such end User by a Partner as a managed service or otherwise (each such Customer, a “Partner”), must comply with this AUP and are expected to adhere to commonly accepted practices of the Internet community. The prohibited uses described below are intended as minimum guidelines regarding improper and inappropriate conduct and should not be interpreted as an exhaustive list. Where a User of a Partner uses any of the Services, such Partner is responsible for compliance by such Users with the requirements of this AUP, the Agreement and Privacy Policy.

2. Prohibited Uses

2.1 The Services may only be used for lawful purposes. Users (including Users of Partner) may not use the Services in any manner in violation of any applicable law or regulation or in any manner that encourages violation of applicable law or regulation, including those set forth in Section 4 of this AUP.

2.2 The Services may not be used 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, a Partner and/or such Customer’s or Partner’s phone numbers. The Services may not be used to contact or allow Users to contact emergency response services.



2.3 The Services may not be used in any manner that causes a telecommunications provider to complain about such use to Act-On or materially violates the following: (i) industry standards, policies and applicable guidelines published by (a) the CTIA (Cellular Telecommunications Industry Association), (b) the Mobile Marketing Association, or (c) any other generally recognized industry associations located anywhere in the world; or (ii) telecommunications provider guidelines and usage requirements as communicated in writing by Act-On to Customer.

2.4 The Services may not be used in a manner which purposely alters or forges any User's identity, deceives any third party or impersonates any other party.

2.5 The Services may not be used to violate system or network security including, but not limited to, by (i) gaining unauthorized access to any User account, network, system, computing facility, equipment, data or information; (ii) engaging in any activities that may interfere with the ability of others to access or use the Services, including, but not limited to 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; (iii) 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 Act-On or any of its other customers; (iv) unauthorized monitoring, including but not limited to recording or monitoring any communication without securing consent from the participants to the communication as required under applicable law; or (v) transmitting files or messages containing computer viruses or propagating worms, Trojan horses, or "spyware" programs.

2.6 Users may not perform any penetration testing or make any other intrusion attempts on the Services without Act-On's prior written consent.

2.7 The Services may not be used to transmit any material, data, or content (a) that infringes the intellectual property rights or other rights of third parties; (b) that is offensive, inappropriate, pornographic, obscene, illegal, or otherwise reasonably objectionable to any person or entity; or (c) 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 Act-On 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.

2.8 Users may not use the Services to harvest or collect information about individuals, including email addresses or phone numbers, (i) without their explicit consent or under



false pretenses or (ii) that infringes the intellectual property rights or other rights of Act-On.

3. Data Types

Users will not upload any of the following types of information: (a) personally identifiable health information, including any information defined as Protected Health Information under Health Insurance Portability and Accountability Act, as amended, (b) drivers license numbers, (c) passport numbers, (d) social security, tax ID or similar numbers, (e) bank, checking, credit card, debit card, or other financial account numbers or (f) any other information or combinations of information that falls within the definition of “special categories of data” under GDPR or “sensitive information” any other applicable law relating to privacy and data protection. Users are solely responsible for compliance with all applicable data privacy and data protection laws in connection with its use of the Services. Any transmission or processing of such information is solely at User’s own risk. Notwithstanding anything herein, in the Agreement or in our Privacy Policy to the contrary, Act-On will have no liability, including, without limitation, any indemnification obligations, whatsoever in connection with any such information transmitted or processed via the Services.

4. Communications Compliance

Act-On expects Users to comply with all applicable laws and industry best practices in connection with their use of the Services, including, without limitation, (i) laws or regulations relating to permissioning and consent requirements pertaining to data acquisition and transmitting email, SMS, MMS, text, and other communications, and (ii) laws or regulations that prohibit engaging in any unsolicited advertising, marketing, messaging or transmission of communications; (iii) anti-spam laws or regulations; or (iv) applicable data protection or privacy laws, regulations, or legislation.

Act-On may provide deliverability services to Users and in connection with such services, may provide Users with consulting and advice regarding deliverability of electronic communications. Notwithstanding the provision of such services and notwithstanding anything herein, in the Agreement or in our Privacy Policy to the contrary, User is responsible for seeking its own legal counsel regarding its compliance with applicable laws, and Act-On shall not be liable for User’s failure or failure of its applicable Partner (as the case may be) to comply with applicable laws even if Act-On has provided consulting and advice regarding deliverability.

4.1 Domestic National Compliance. Users agree to adhere to the sender requirements and obligations under the CAN-SPAM act of 2003 and any amendment or successor thereto. Additionally, Users must abide by the Telephone Consumer Protection Act, as amended (TCPA), and the Children’s Online Privacy Protection Act as they pertain to Users marketing and prospecting using the Services.



4.2 State Laws. Users also agree to abide by any existing state laws regarding transmission of electronic communications including, but not limited to, those that specifically address sending email, text and other electronic communications to minors.

4.3 International Compliance. Users agree that sending email(s), SMS, MMS, text messages and other electronic communications to international countries will require it to abide by and comply with the “destination country” laws and other compliance requirements for commercial electronic transmissions and communications. For purposes of clarity, Act-On expects Users to agree to the laws of the countries where the recipients of its transmissions and communications are located when such transmissions are received.

4.4 Content (Line of Business) Performance Acknowledgement; Role-Based Email. User acknowledges that certain forms of email and messaging content can cause deliverability issues, and User is entirely responsible for managing its email, messaging and other electronic communications content. Without limitation and by way of example only, messaging with content containing products and services that are illegal for minors to purchase have been known to be high in performance related issues. Users may not use the Services to send emails to role-based email addresses.

4.5 Volume Management. In order to proactively manage a frequency reputation a “volume cap” of ten emails or text messages per contact per month will be enforced on an account basis.

4.6 Unsolicited Communications. The Services may not be used by Users to send any unsolicited, unwanted, or harassing communications (commercial or otherwise) or any Unsolicited Commercial Emails or Text Messages (as defined below) or other similar phone calls, SMS or MMS messages, chat, voice mail, video, email, fax or other communication. As used in this AUP, “Unsolicited Commercial Email or Text Messages” is defined as email or SMS, MMS, text messages or other electronic communication sent to individuals who (i) do not have a pre-existing relationship with User and (ii) have not provided consent to the receipt of such emails or text messages, including express or affirmative consent, double-out-in and/or parental consent where required by law.

4.7 Required Practices. Users must comply with the practices in this Section 4.7. Instances of noncompliance may result in access to the Services being suspended or terminated. The Services may not be used in a way that violates generally recognized industry guidelines, including, without limitation:

- (i) **Consent.** Users must obtain consent from any individual to whom it wishes to send commercial emails or text messages, for the type of messages that Users wishes to send, and maintain a record of such consent, including express consent where required by law. Such consent does not permit messages from other brands, or permit messaging for other purposes or



uses. Upon request of Act-On, Users will provide documentation evidencing that it obtained any and all consents required by applicable law.

- (ii) **Age and Content Requirements.** Users must ensure that with respect to its messages that (a) no message recipient is younger than the legal age of consent based on where the recipient is located; and (b) the message content complies with all applicable laws of the jurisdiction in which the message recipient is located.
- (iii) **Non-Permission Lists.** Users will not use non-permission based email or phone lists (i.e., lists in which each recipient has not explicitly granted permission to receive emails, text or other electronic communications from Users by affirmatively opting-in to receive such communications, as required by law).
- (iv) **Messaging Limitations.** Notwithstanding the above, Users may send an outbound message to an individual in response to a message from that individual or to provide information requested by the individual (e.g., password requests and appointment reminders). Users may not reply to such requests with promotional or marketing content.
- (v) **Email-Specific Practices.**
 - a. **Email Recipients.** Users may not (i) use third-party email addresses, domain names, or mail servers without proper permission; (ii) send emails to non-specific addresses (e.g., webmaster@domain.com or info@domain.com); and (iii) send 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).
 - b. **Unsubscribe.** Users may not (i) fail to include a working “unsubscribe” link in each commercial email (i.e. non-transactional) that allows the recipient to remove themselves from User’s mailing list unless the communication is i; and (ii) fail to comply with any request from a recipient to be removed from User’s mailing list within 10 days of receipt of the request.
 - c. **Other Email Practices.** Users may not (i) fail to include in each commercial email a link to the then-current privacy policy applicable to that email; (ii) disguise the origin or subject matter of any email or falsify or manipulate the originating email address, subject line, headers, or transmission path information for any email; (iii) fail to include in each



commercial email, Users' valid physical mailing address or a link to that information; and (iv) include "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.

- (vi) **SMS, MMS, Text and Other Electronic Communication-Specific Requirements.**
 - a. **Recycled Phone Numbers.** In the event that any individual who has previously opted in or consented to receiving emails or text messages changes or deactivates their mobile telephone number, Users agree it will promptly update such information to ensure that its messages are not sent to the person that acquires the old number.
 - b. **Initial SMS, MMS and Text Message Content.** The initial message of each conversation must clearly identify User as the source of the message, and include the following language: "Reply STOP to unsubscribe," or the equivalent using another standard opt-out keyword, such as OPT OUT.
 - c. **Revocation of Consent.** Individuals must also have the ability to revoke consent at any time by replying with a standard opt-out keyword. When an individual opts out, Users who were the source of the message may not send any further messages other than a confirmation of the opt-out.
- (vii) **Configurations.** Each User must ensure that it properly configures the communications functionality within the Services to comport with best practices as directed by Act-On.

5. Customer's Responsibilities and Act-On's Rights

Users will cooperate with appropriate law enforcement and other governmental agencies and other parties involved in investigating claims of illegal or inappropriate activity. If any Users become aware of any violation of this AUP by any person, including, but not limited to, downstream customers, User, or third parties, Act-On requires that such Users notify Act-On immediately at support@act-on.com or privacy@act-on.com. Recipients of messages sent using any Services are also encouraged to report suspected violations of this AUP by forwarding a copy of the applicable email to abuse@act-on.net. Act-On will catalog, investigate and address all reports of violations and/or abuse. In addition to other remedies available pursuant to the Agreement, any Users account found to be in violation of this AUP is



subject to immediate suspension and will not be allowed to send any communications using the Services. In such event, access will only be restored when Act-On is satisfied that such violation has been remedied. Users are strictly responsible for all use of the Services in violation of this AUP, including, but not limited to, use by applicable Users, including Users of Partners. Where a Partner (or Partner's End User, as defined in the applicable Partner Agreement) uses any of the Services, End User and such Partner will be jointly and severally responsible for the acts and omissions of such End Users, including, but not limited to, their noncompliance with and breach of this AUP.

6. Generative AI.

As a feature of the Service, Act-On may make generative artificial intelligence/machine learning tools available within the Service ("AI Feature"). The AI Feature is made available to assist Users with drafting email content and for no other purpose. Users use the AI Feature at their own risk. Users are prohibited from inputting any third party's confidential or proprietary information into the AI Feature. Users should be aware that the Act-On makes no representation or warranty with respect to the AI Feature and that any information inputted into the AI Feature is not considered confidential information. Users are prohibited from inputting personally identifiable information into the AI Feature unless Customer has provided all legally required disclosures and obtained any legally required consents. Notwithstanding the foregoing, Users are prohibited from inputting any of the data types described in Section 3 into the AI Feature.