Act-On Software, Inc.
Act-On Acceptable Use Policy

This Acceptable Use Policy ("**AUP**") establishes rules and requirements for use of Act-On Software, Inc.'s ("**Act-On**") websites, products and services, including any AI Features, add-ons and modules made available by Act-On (collectively, the "**Services**"). This AUP is incorporated by reference into the definitive agreement between Act-On and the Customer regarding such Services ("**Agreement**"). Act-On may update this AUP from time to time by posting an updated version at https://www.act-on.com/legal, provided that any update that materially diminishes Customer's rights or materially increases Customer's obligations will not apply during an existing Subscription Term unless required by applicable law, required by a telecommunications provider or Third-Party AI Service provider, or reasonably necessary to address an Actionable Threat, abuse of the Services, security risk, deliverability risk, or violation of applicable law. Capitalized terms not defined in this AUP will have the meanings set forth in the Agreement.

1. Compliance
This AUP is intended to protect Act-On, Customers, Users, Recipients, telecommunications providers, Third-Party AI Service providers, and the Internet community as a whole from improper, inappropriate, abusive, or illegal activity. When using any Act-On Services, Customer and all persons or entities that access or use the Services through Customer's account, including Customer's designated users, Agency customers, downstream customers, managed service customers, representatives, contractors, agents and Recipients (collectively, "Users"), must comply with this AUP and are expected to adhere to commonly accepted practices of the Internet community. The prohibited uses described below are minimum guidelines regarding improper and inappropriate conduct and should not be interpreted as an exhaustive list. Customer is responsible for all acts and omissions of its Users and for ensuring that all Users comply with this AUP, the Agreement, the DPA, the Documentation, the Privacy Policy, and any applicable Order Form.

2. Prohibited Uses
2.1 The Services may only be used for lawful purposes. Users may not use the Services in any manner that violates, facilitates violation of, or encourages violation of any applicable law, rule or regulation, the Agreement, the DPA, the Documentation, this AUP, any Order Form, or any telecommunications provider, app store, browser, email service provider, domain registrar, registry, or other third-party platform requirements applicable to the Services, 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, telecommunications provider, email service provider, domain registrar, registry, or other third-party platform to request suspension, blocking, filtering, throttling, delisting, takedown, quarantine, or other restriction of the Services, Customer's account, any User's account, any sending domain, or any phone number. 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, email service provider, domain registrar, registry, browser, app store, Third-Party AI Service provider, or other third-party platform to complain about such use to Act-On or that 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, (c) M3AAWG, (d) The Campaign Registry or any successor registry or verification body, or (e) any other generally recognized industry association or standards body located anywhere in the world; (ii) telecommunications provider, email service provider, domain registrar, registry, browser, app store, Third-Party AI Service provider, or other third-party platform guidelines and usage requirements as communicated in writing by Act-On to Customer; or (iii) any applicable sender authentication, campaign registration, toll-free verification, 10DLC, short code, domain authentication, or similar requirements.

2.4 The Services may not be used in a manner that alters, masks, spoofs, or forges any User's identity, sending domain, caller ID, email header, transmission path, originating number, brand, campaign, or other source identifier, 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, security, integrity, or stability of the Services; (iii) attempting to bypass, disable, interfere with, or break any security, rate limit, filtering, authentication, authorization, monitoring, abuse-prevention, or usage control 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, its vendors, its customers, or Recipients; (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; (v) transmitting files or messages containing computer viruses or propagating worms, Trojan horses, ransomware, malware, spyware, or other harmful code; or (vi) attempting to probe, scan, or test the vulnerability of the Services except as expressly permitted under Section 2.6.

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, generate, store, process, display, or distribute any material, data, Input, Output, or content (a) that infringes, misappropriates, or violates the intellectual property, privacy, publicity, confidentiality, contractual, or other rights of any third party; (b) that is offensive, inappropriate, pornographic, obscene, exploitative, illegal, deceptive, fraudulent, or otherwise reasonably objectionable to any person or entity; (c) that is, facilitates, or encourages libelous, defamatory, discriminatory, threatening, abusive, harassing, 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; or (d) that promotes or facilitates illegal drugs, controlled substances, cannabis, CBD, tobacco, vaping, weapons, payday lending, credit repair, counterfeit goods, human trafficking, sexual exploitation, or other content categories prohibited by applicable law, telecommunications provider policies, email service provider policies, CTIA guidelines, or other third-party platform requirements as such may be updated from time to time.

2.8 Users may not use the Services to harvest, scrape, purchase, rent, collect, verify, enrich, append, or otherwise obtain information about individuals, including email addresses, phone numbers, device identifiers, or other Personal Data, (i) without all rights, notices, consents, lawful bases and permissions required by applicable law; (ii) under false pretenses; (iii) in violation of any website terms, privacy notice, platform policy, or opt-out, sale, share, targeted advertising, cross-context behavioral advertising, do-not-call, or similar privacy preference; or (iv) in a manner that infringes the intellectual property rights or other rights of Act-On or any third party.

2.9 Users may not use the Services to engage in spam, phishing, pharming, smishing, vishing, credential harvesting, malware distribution, lead generation fraud, affiliate abuse, list bombing, spam trap seeding, evasion of filters or rate limits, snowshoeing, traffic pumping, artificial inflation of traffic, generation of misleading engagement metrics, or other abusive or deceptive activity. Users may not use the Services to avoid detection, distribute substantially similar content across multiple accounts, domains, numbers, brands, or campaigns in a manner intended to bypass Act-On's or a third party's restrictions, or continue sending to Recipients who have opted out, complained, bounced, or otherwise indicated that messages are unwanted.

2.10 Users may not access or use the Services to directly or indirectly develop, train, promote, distribute, sell, or support any product or service that competes with the Services, to copy any feature, function, user interface,

workflow, or Documentation, or to publish or disclose any benchmark, performance, security, or availability results without Act-On's prior written consent.

3. Data Types
Users will not upload, submit, transmit, store, process, or make available through the Services any of the following types of information: (a) protected health information, health information, medical records, or information subject to HIPAA or similar health privacy laws; (b) driver's license numbers, passport numbers, government identification numbers, social security numbers, tax identification numbers, national insurance numbers, or similar identifiers; (c) bank, checking, credit card, debit card, payment card, financial account, authentication credential, password, security question, private key, or similar financial or account access information; (d) biometric identifiers, genetic data, precise geolocation data, criminal history, children's data, or data concerning minors; (e) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, immigration status, or citizenship status; or (f) any other information or combination of information that falls within the definition of "special categories of data," "sensitive personal information," "sensitive data," "consumer health data," or similar terms under applicable Data Protection Laws or other applicable privacy or data protection laws (collectively, "Prohibited Data"), unless Act-On expressly agrees in writing that the applicable Services may be used to process such Prohibited Data. Users are solely responsible for compliance with all applicable data privacy and data protection laws in connection with their use of the Services. Any transmission or processing of Prohibited Data not expressly authorized by Act-On in writing 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 Prohibited Data transmitted or processed via the Services without Act-On's express written authorization.

4. Communications Compliance
Act-On expects Users to comply with all applicable laws, industry best practices, Documentation, and third-party platform requirements in connection with their use of the Services, including, without limitation, (i) laws or regulations relating to permissioning, lawful basis, notice, consent, opt-in, opt-out, and revocation requirements pertaining to data acquisition and transmitting email, SMS, MMS, text, voice, chat, push, and other communications; (ii) laws or regulations that prohibit unsolicited advertising, marketing, messaging, or transmission of communications; (iii) anti-spam, telemarketing, call recording, biometric, consumer protection, and unfair or deceptive practices laws or regulations; and (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, recommendations, configuration guidance, 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 determining and documenting its own compliance with applicable laws, provider requirements, and industry standards, and Act-On shall not be liable for User's failure or the failure of any User, Agency customer, downstream customer, or managed service customer to comply with applicable laws, provider requirements, or industry standards even if Act-On has provided consulting, recommendations, configuration guidance, or 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), the Telemarketing Sales Rule, the Children's Online Privacy Protection Act, the FTC Act, applicable FCC and FTC rules and guidance, and any other federal laws or regulations that apply to Users' marketing, prospecting, data collection, communications, or use of the Services.

4.2 State Laws. Users also agree to abide by any existing state laws regarding transmission of electronic communications, telemarketing, do-not-call requirements, automatic dialing, call recording, consumer privacy, consumer health data, unfair or deceptive practices, age-restricted content, and communications to minors,

including, but not limited to, laws that specifically address sending email, text and other electronic communications to minors.

4.3 International Compliance. Users agree that sending emails, SMS, MMS, text messages, voice messages, chat messages, push notifications and other electronic communications to recipients in countries outside the United States requires Users to abide by and comply with the "destination country" laws and other compliance requirements for commercial electronic transmissions and communications, including Canada's Anti-Spam Legislation, the EU ePrivacy Directive, the UK Privacy and Electronic Communications Regulations, GDPR, UK GDPR, and similar laws where applicable. For purposes of clarity, Act-On expects Users to comply with 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, messaging, and AI-generated content can cause deliverability, carrier filtering, blocking, complaint, and regulatory 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 age-restricted products or services, financial products, employment opportunities, lead generation, affiliate marketing, contests, sweepstakes, health claims, or products and services that are illegal for minors to purchase can be high in performance related issues. Users may not use the Services to send emails to role-based email addresses, including addresses such as abuse@, admin@, info@, privacy@, sales@, security@, support@, or webmaster@.

4.5 Volume Management. In order to proactively manage frequency, sender reputation, carrier throughput, provider restrictions, and Recipient experience, Act-On may enforce volume, frequency, rate, throughput, domain, campaign, number, Recipient, or account-level caps or throttling, including a volume cap of ten emails or text messages per contact per month on an account basis, unless otherwise approved by Act-On in writing.

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, push notification, or other communication. As used in this AUP, "Unsolicited Commercial Email or Text Messages" means email, 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 communications, including express consent, prior express written consent, affirmative consent, one-to-one consent, double opt-in and/or parental consent where required by law, provider requirements, or industry standards.

4.7 Required Practices. Users must comply with the practices in this Section 4.7 and any additional consent, registration, authentication, suppression, opt-out, and sender reputation practices communicated by Act-On in the Documentation or in writing. Instances of noncompliance may result in access to the Services being suspended or terminated in accordance with the Agreement. The Services may not be used in a way that violates generally recognized industry guidelines, including, without limitation:

(i) **Consent.** Users must obtain and maintain all consents, lawful bases, notices, disclosures, opt-ins, authorizations and permissions required to send commercial emails, text messages, voice messages, chat messages, push notifications, and other communications to each Recipient, for the specific sender, brand, campaign, purpose, channel, message type, and frequency used by User, including express consent, prior express written consent, one-to-one consent, affirmative consent, double opt-in and/or parental consent where required by law, provider requirements, or industry standards. Such consent does not permit messages from other brands, or permit messaging for other purposes, channels, campaigns, frequencies, or uses. Upon request of Act-On, Users will promptly provide documentation evidencing that they obtained and maintained any and all consents required by applicable law, provider requirements, and industry standards.

(ii) **Age and Content Requirements.** Users must ensure that with respect to their messages that (a) no message recipient is younger than the legal age of consent or the minimum age permitted to receive the applicable message content based on where the recipient is located; (b) the message content complies with all applicable laws of the jurisdiction in which the message recipient is located; and (c) the message content complies with applicable provider requirements, industry standards, and any age-gating, consent, and content restrictions communicated by Act-On.

(iii) **Non-Permission Lists.** Users will not use non-permission based email, phone, device identifier, or other contact lists, including purchased, rented, scraped, harvested, appended, co-registration, affiliate, lead-generation, or shared lists, unless each recipient has granted all permissions required by applicable law, provider requirements, and industry standards to receive the applicable emails, text messages, or other electronic communications from the specific User, brand, campaign, purpose, channel, message type, and frequency used by User.

(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, account notices, confirmations and appointment reminders), only to the extent permitted by applicable law, provider requirements, and industry standards. Users may not reply to such requests with promotional or marketing content unless the User has obtained all legally required consents for such promotional or marketing content.

(v) **Email-Specific Practices.**

a. **Email Recipients.** Users may not (i) use third-party email addresses, domain names, sending domains, authentication records, or mail servers without proper permission; (ii) send emails to non-specific, group, distribution, or role-based addresses (e.g., webmaster@domain.com or info@domain.com); (iii) send emails to spam traps, seed lists, suppressed contacts, opted-out Recipients, purchased lists, or addresses obtained through harvesting, dictionary attacks, scraping, or automated means; or (iv) send emails that result in an unacceptable number of spam, abuse, bounce, blocklist, 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, list-unsubscribe mechanism, or other legally compliant opt-out mechanism in each commercial email (i.e. non-transactional) that allows the recipient to remove themselves from User's mailing list; (ii) require a recipient to pay a fee, provide information other than an email address, log in, or take more than the minimum steps permitted by applicable law to submit an unsubscribe request; or (iii) 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 or any shorter period required by applicable law, provider requirements, or industry standards.

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, authentication records, 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; (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; or (v) fail to comply with applicable sender authentication, domain alignment, bounce processing, suppression, blocklist remediation, and sender reputation

requirements communicated by Act-On or required by email service providers, mailbox providers, or industry standards.

(vi) SMS, MMS, Text, Voice, Chat, Push 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, text messages, or other communications changes, ports, or deactivates their mobile telephone number, Users agree they will promptly update such information and use commercially reasonable practices designed to ensure that 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 all disclosures required by applicable law, provider requirements, and industry standards, including, as applicable, program name, message frequency, "message and data rates may apply," customer care or HELP instructions, and 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 or any other reasonable method required by applicable law, provider requirements, or industry standards. Users must recognize and honor opt-out keywords and requests, including STOP, STOPALL, UNSUBSCRIBE, CANCEL, END, QUIT, REVOKE, and OPT OUT, within the time required by applicable law, provider requirements, or industry standards. When an individual opts out, Users who were the source of the message may not send any further messages other than a single confirmation of the opt-out, except to the extent a subsequent message is legally permitted and supported by separate consent or another lawful basis.

(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, including suppression, opt-out, consent, authentication, registration, verification, frequency, throttling, bounce processing, complaint processing, and unsubscribe settings.

(viii) Registration and Verification. Users must complete and maintain all brand, campaign, number, domain, sender, toll-free, 10DLC, short code, RCS, caller ID, and similar registration, verification, authentication, and approval requirements applicable to their use of the Services. Users may not send communications that materially deviate from the approved or registered use case, sender identity, message samples, call-to-action, opt-in flow, campaign description, or message frequency.

(ix) Messaging Content Restrictions. Users may not use SMS, MMS, text, voice, chat, push, or other electronic communication functionality to send content prohibited by applicable law, provider requirements, CTIA guidelines, or other industry standards, including content involving sex, hate, alcohol, firearms, tobacco, vaping, cannabis, CBD, controlled substances, gambling, payday loans, debt relief, credit repair, phishing, smishing, lead generation fraud, or content that is false, deceptive, misleading, or likely to generate complaints, blocking, filtering, or enforcement.

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

Users will cooperate with Act-On, appropriate law enforcement and other governmental agencies, telecommunications providers, email service providers, domain registrars, registries, Third-Party AI Service providers, and other parties involved in investigating claims of illegal, inappropriate, abusive, or noncompliant

activity. If any Users become aware of any violation of this AUP by any person, including, but not limited to, downstream customers, Users, 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 may catalog, investigate and address all reports of violations and/or abuse. In addition to other remedies available pursuant to the Agreement, Act-On may suspend, limit, throttle, block, quarantine, reject, remove, disable, or terminate access to or use of the Services, Customer's account, any User's account, any sending domain, any phone number, any campaign, any AI Feature, or any communication if Act-On reasonably determines that Customer or any User has violated this AUP or that the activity exposes Act-On, its vendors, its customers, Recipients, or third parties to an Actionable Threat or other security, legal, operational, deliverability, reputational, regulatory, or material business risk. Act-On will provide advance notice prior to any suspension where reasonably practicable, except where Act-On reasonably determines that immediate action is necessary to prevent or mitigate an Actionable Threat, abuse, security incident, provider enforcement, legal violation, or other material risk. In such event, access will only be restored when Act-On is satisfied that the violation or risk has been remedied. Customer is strictly responsible for all use of the Services in violation of this AUP, including use by all Users, Agency customers, downstream customers, managed service customers, representatives, contractors, and agents. Where an Agency customer, downstream customer, managed service customer, or other User uses any of the Services through Customer's account, Customer will be responsible for the acts and omissions of such Users, including, but not limited to, their noncompliance with and breach of this AUP.

7. Relationship to Agreement and DPA.

This AUP is part of the Agreement. In the event of a conflict between this AUP and the Agreement, the Agreement will control, except that this AUP will control with respect to acceptable use, abuse prevention, prohibited content, prohibited data types, communications compliance, sender reputation, provider requirements, and Act-On's enforcement rights relating to the foregoing. In the event of a conflict between this AUP and the DPA, the DPA will control with respect to Act-On's processing of Customer Personal Data. Nothing in this AUP limits Customer's obligations under the Agreement or the DPA, including Customer's responsibility for Customer Content, Inputs, Outputs, Users, Recipients, notices, consents, lawful bases, and compliance with applicable laws.