Version Dated: June 30, 2025

EMAIL MARKETING ACCEPTABLE USE POLICY

This Email Marketing Acceptable Use Policy ("**EMAUP**") sets forth additional terms under which customers may use Treasure Data's Email Marketing service (the "**Engage Service**") identified on an Order Form as part of the Engage Studio or equivalent and forms part of the applicable Treasure Data Terms of Service ("**Terms of Service**"), master service agreement, Order Form and/or other agreement ("**Service Agreement**") that governs the purchase of cloud services ("**Service**") provided by Treasure Data, Inc. ("**Treasure Data**") to the customer thereunder ("**Customer**"). Compliance with this EMAUP protects the interests of Message Recipients, Treasure Data, and its customers.

1. DEFINITIONS

For the purposes of this EMAUP, the following capitalized words are ascribed the following meanings. All capitalized terms not defined in this EMAUP shall have the meaning ascribed to them in the Terms of Service, or if a Service Agreement applies, the substantially equivalent terminology defined therein:

1.1 "**Content Editor**" refers to a tool powered by Beefree SDK that enables users to create and edit marketing content such as emails within the Engage Service.

1.2 "**Recipient**" refers to any individual to whom a Message is sent using the Engage Service.

1.3 "**Message**" refers to any email or other electronic message sent through the Engage Service.

2. GENERAL PROHIBITIONS

2.1 Customer must not use the Engage Service to:

2.1.1 Send any content that is threatening, abusive, harassing, defamatory, deceptive, fraudulent, obscene, indecent, or illegal;

2.1.2 Misrepresent or obscure their identity, including through the use of forged headers or misleading subject lines;

2.1.3 Transmit sensitive information, including but not limited to financial account details, government IDs, payment card information, medical information, or children's personal information;

2.1.4 Send Messages that result in excessive spam or complaints, bounces, spam trap hits, unsubscribes, blocklistings, or other poor deliverability outcomes (even if the Messages themselves are not actually spam); or

2.1.5 Employ sending practices that negatively impact Treasure Data or its customers.

3. EMAIL MARKETING SPECIFIC POLICIES

3.1 Customer's Compliance with the Law and List Management.

3.1.1 Customer shall ensure its use of the Engage Service complies with all applicable laws, including any applicable data protection and privacy laws. Without limiting the foregoing, Customer must ensure that:

(ai) any necessary consent is obtained from Recipients for sending them Messages and for the processing of their Personal Data as part of the use of the Engage Service by Customer, and/or any necessary privacy notice is provided to Recipients in accordance with the requirements of applicable law;

(b) any necessary consent is obtained from Recipients according to the requirements of applicable law (including for example the European Directive 2002/58/EC (ePrivacy) as amended by Directive 2009/136/EC and implementing national legislation, where applicable) for tracking Recipients' engagement with Messages (for example, through the use of tracking devices) according to the Documentation related to the Engage Service and any configuration set by Customer.

Customer must produce evidence of compliance with this section upon Treasure Data's request.

3.1.2 Customer is solely and exclusively responsible for determining or reviewing the content of any Message, the list of the intended recipients of any Message and the criteria for inclusion of email addresses in any applicable suppression list.

3.1.3 Customer must not send Messages to: (a) purchased, rented, or appended lists; (b) Message addresses scraped from the internet or programmatically generated; (c) Role-based or non-specific addresses (e.g., info@domain.com); (d) Distribution lists or listservers; or (e) devices or Recipients as SMS/MMS or text messages.

3.1.4 Customer must maintain accurate and up-to-date mailing lists.

3.1.5 Customer acknowledges and agrees that when (a) a User uses the Engage Service or (b) the Content Editor is used, a third party called BEE Content Design, Inc., which provides the BeeFree SDK, will process Users' IP Addresses (in the event of (a)) or Recipients' IP addresses (in the event of (b)) in the capacity of an independent "data controller" according to its privacy policy, for the purposes of managing debugging activities, collecting information about how their software is used and preventing and identifying any abuse in the use of their software or any other fraudulent activity. The processing of such IP addresses includes without limitation their temporary storage in the EU.

3.1.6 Customer must have a publicly available privacy policy covering the processing of Personal Data in connection with Customer's use of the Engage Service and Content Editor that complies with applicable laws.

3.2 Content Requirements

3.2.1 All Messages must accurately identify Customer or its Affiliates or related parties as the sender and must not contain or link to any malicious content, including phishing sites, pyramid schemes, or affiliate marketing content without explicit permission.

3.2.2 Subject lines must not be deceptive or misleading.

3.2.3 Customer shall not display on any Messages any content that violates the intellectual property rights or other rights of third parties (e.g., trademarks, confidentiality, publicity or privacy rights) or applicable laws.

3.3 Unsubscribe Mechanism

3.3.1 All Messages must include a clear, conspicuous, and functional unsubscribe mechanism.

3.3.2 Unsubscribe requests must be honored promptly, and within legally required timeframes.

3.3.3 Customer must not send further Messages to unsubscribed Recipients unless new consent is obtained.

4. TECHNICAL USAGE AND SECURITY

4.1 Customer must not exceed their entitled usage limits identified in the Order Form or attempt to process more data than reasonably expected based on their package.

4.2 Customer must not engage in activities that may threaten the security, stability, or availability of the Engage Service, including but not limited to: (a) overwhelming Treasure Data's infrastructure with unreasonable loads; (b) attempting to probe, scan, or test the vulnerability of the Engage Service; or (c) accessing the Engage Service through unsupported interfaces.

5. COMPLIANCE AND ENFORCEMENT

5.1 Treasure Data reserves the right to monitor compliance with this EMAUP. Regardless, Treasure Data is not responsible for determining or reviewing the content of any Message or the list of intended recipients of any Message.

5.2 Violations of this EMAUP may result in suspension or termination of the Customer's access to the Engage Service.

5.3 Treasure Data will provide a written basis for any suspension or termination.

6. UPDATES TO THE POLICY

6.1 Treasure Data reserves the right to update this EMAUP from time to time in accordance with industry best practices and applicable law, and in order to reflect any change to the Engage Service, its functionalities and capabilities. Any changes to this EMAUP will be effective 30 days after publication of the updated version on Treasure Data website, or 30 days after its written communication to Customer.