Acceptable Use Policy

Last Updated: 01.06. 2024

Our customers rely on Replenit to keep the Replenit Services running without disruption and to provide guidance on legal requirements and industry best practices.

This Acceptable Use Policy (“AUP”) sets forth how the Replenit Services must be used, and more importantly, what constitutes misuse of the Replenit Services, either because the activity violates applicable law, or because it poses a risk to the Replenit Services. Terms used herein without definition are defined in the subscription agreement (“Agreement”) in place between Replenit (or a Replenit Reseller) and its customers.

Updates to the AUP: Replenit reserves the right to update this AUP in accordance with industry best practices and applicable law by posting a revised copy on this webpage.

AUP violations: A violation of this AUP shall be deemed a breach of the Agreement and may result in Replenit’s refusal to send Messages or in the suspension and/or termination of Customer’s subscription to use the applicable services.

Replenit will provide a written basis for any suspension or termination.

1. MESSAGING POLICY

1.1 Messaging includes sending email messages, SMS/MMS messages, and any other electronic messages through Replenit Services. All Messages sent via the Replenit through your integrated Third-Party Provider services must comply with applicable laws, applicable.

1.2 All messages could only be sent to the consented, according to the respective laws. , recipients

1.3 All related channels/messages must include a visible and working unsubscribe mechanism that complies with industry best practices.

1.4 Messages may not:

(i) Disguise the origin or subject matter of the message, or contain a falsified or manipulated “from” address, subject line, header, or transmission path information; and

(ii) Contain links to phishing sites or content related to pyramid schemes, multi-level marketing opportunities, affiliate marketing, or any other content that is reasonably likely to be tortious, libelous, deceptive, fraudulent, infringing, harassing, harmful, obscene, or abusive (“Malicious Content”).

(iii) Customer must have a publicly-available privacy policy for all active sending domains that complies with applicable laws and Third-Party Provider terms of use.

2. REASONABLE USAGE

If Customer exceeds its entitlements or attempts to process more data through the Replenit Services than reasonably expected based on Customer’s entitlements and package (e.g., abusive data processing or unduly burdensome data processing through the Replenit Services), Replenit may manage data processing traffic in order to preserve the overall stability of the Replenit Services.

3. PROHIBITED ACTIVITIES

3.1 Customers shall not take actions that may threaten the security, stability, or availability of the Replenit Services, including:

(a) Overwhelming the Replenit infrastructure by imposing an unreasonably large load on the Replenit Services (i.e., using “robots,” “spiders,” “offline readers,” or other automated systems to send more request messages to the Replenit
(b) Services than a human could reasonably purchase in the same period of time by using a normal browser);

3.2 Going beyond the use parameters for any given product or feature, as described in the Documentation;

3.3 Accessing any part of the Replenit Services by any means other than our publicly-supported interfaces (for example,“scraping”).

4. EXTERNAL-FACING SERVICES

4.1 Customer shall not display on any external-facing Replenit Services any Malicious Content and/or content that violatesthe intellectual property rights or other rights of third parties (such as confidentiality, publicity or privacy rights) or applicable laws.

4.2 Customer shall identify itself clearly as the recipient of any data or information collected by Customer through any external-facing Replenit Services.