Privacy Policy & Data Processing Addendum (Non-GDPR)

Effective 4 Nov 2026

This Privacy Policy and Data Processing Addendum (“Privacy & DPA”) describes how the Company collects, uses, processes, retains, and protects data in connection with the operation of the Platform. This document forms part of the Master Subscription Agreement (“Agreement”) between the Company and the Customer.

This Privacy & DPA is designed for a non-EU, non-GDPR context and reflects generally accepted data protection principles applicable to commercial SaaS platforms. Where applicable law requires additional obligations, the Company may supplement or amend this document accordingly.

1. Roles and Scope

For purposes of data processed through Campaigns, Customer acts as the data controller with respect to Campaign data and end-user data collected through Campaigns. The Company acts as a data processor or service provider, processing data on Customer’s behalf in connection with providing the Platform and in accordance with Customer’s instructions as reflected in the use of the Platform.

This Privacy & DPA applies to all personal data processed by the Company in connection with Customer’s use of the Platform, whether during exploratory use, testing, or active Campaigns.

2. Categories of Data Processed

Depending on Customer’s configuration of Campaigns, the Platform may process the following categories of data:

- Campaign configuration data and metadata;
- End-user interaction data generated through Campaign participation;
- Personal data submitted by end users as part of a Campaign;
- Technical and usage data relating to access and operation of the Platform.

The Company does not determine the specific categories of personal data collected through Campaigns and does not control or verify the content or legality of such data. Customer determines and is responsible for the categories of personal data collected through Campaigns.

3. Purpose and Instructions for Processing

The Company processes data for the purpose of providing, operating, supporting, securing, and improving the Platform and related Services.

Customer instructs the Company to process data by configuring and operating Campaigns through the Platform. Customer is responsible for ensuring that its instructions comply with applicable data protection laws.

4. Data Retention and Deletion

Campaign-related data is retained for a limited period following the expiration of a Campaign, as described in the applicable service description or Pricing Terms.

Unless otherwise agreed, Campaign data is retained for up to seven (7) days following Campaign expiration, after which such data may be deleted or anonymized as part of the Company's normal data management practices.

In certain cases, limited copies of such data may remain in system backups or logs for security, legal, or operational reasons until such records are overwritten or otherwise removed in the ordinary course of system operations.

Extended data retention options may be offered subject to applicable pricing terms.

The Company reserves the right to update data retention periods and practices from time to time on a prospective basis.

5. Security Measures

The Company implements reasonable technical and organizational measures designed to protect data against unauthorized access, loss, misuse, or disclosure, taking into account the nature of the data and the risks involved.

Such measures may include access controls, encryption in transit, monitoring, and internal security policies. The Company does not guarantee absolute security.

6. Sub-Processors

The Company may engage its affiliates or third-party service providers (sub-processors) to assist in providing the Services, such as cloud infrastructure, development support, analytics, or communications providers.

The Company remains responsible for the acts and omissions of its sub-processors in accordance with this Privacy & DPA.

The Company and its sub-processors may process personal data in jurisdictions where they operate.

A list of current sub-processors may be made available upon request or through the Platform.

7. Customer Obligations

Customer is responsible for:

- providing all required notices and obtaining any necessary consents from end users;
- ensuring that data collected through Campaigns is lawful, relevant, and limited to the intended purpose;
- responding to end-user requests relating to personal data, including access or deletion requests.

The Company does not independently respond to end-user data subject requests except as required by applicable law, but may reasonably assist Customer in responding to such requests where appropriate.

8. Data Transfers

Data processed through the Platform may be processed by the Company and its affiliates in various jurisdictions.

The Company will take reasonable steps to ensure that such transfers are conducted in accordance with applicable data protection laws.

9. Audits and Compliance

Customer may request reasonable high-level information regarding the Company's data protection practices to verify compliance with this Privacy & DPA.

The Company is not obligated to provide on-site audits or respond to detailed questionnaires unless otherwise agreed.

10. Incident Management

The Company maintains internal procedures to address data security incidents.

The Company does not commit to specific notification timelines but will use reasonable efforts to notify Customer of material data security incidents affecting Campaign data within a commercially reasonable timeframe after becoming aware of such incident, taking into account the nature of the incident, operational impact, and available resources.

11. Updates to this Privacy & DPA

The Company may update this Privacy & DPA from time to time in accordance with the update provisions set forth in the Master Subscription Agreement (MSA).

End of Privacy Policy & Data Processing Addendum