Data processing addendum (DPA)

Last updated: [Date]

This Data Processing ADDENDUM ("DPA" or "DPA") is entered into between BOTTO PLATFORM - FZCO (license no. 27443) ("Data Processor") and the User ("Data Controller") and forms an integral part of the User Agreement ("Agreement").

By using the Service, the Data Controller agrees to the terms of this DPA.

1. TERMS AND DEFINITIONS

The terms used in this DPA have the meanings defined in the Agreement and UAE Federal Law No. 45 of 2021 ("PDPL"). The terms "Data Controller," "Data Processor," "Data Subject," "Processing," "Personal Data," and "Special Categories of Data" shall be interpreted in accordance with the PDPL.

Data Breach: a security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

Technical and Organizational Measures: measures designed to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

2. SCOPE AND PURPOSES OF PROCESSING

2.1. The Data Processor undertakes to process Personal Data exclusively on behalf of and at the direction of the Data Controller, in strict accordance with the terms of the Agreement, these Terms, and the Data Controller's written instructions set out in its Privacy Policy and the Service settings.

2.2. Purposes of Processing: Processing is carried out solely for the purposes of providing the Service, including making automated voice calls and sending text messages as instructed by the Data Controller, as well as to ensure technical support and security of the Service.

2.3. Nature of processing: collection, recording, organization, structuring, storage, adaptation, modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.4. Categories of Data Subjects: individuals (end recipients) whose contact information is provided by the Data Controller for use of the Service.

2.5. Types of Personal Data processed: Contact information (phone numbers, email addresses), content of voice and text messages, communication metadata (time, date, duration).

2.6. Prohibition on processing Special Categories of Data: The Data Processor expressly prohibits the Data Controller from uploading or processing any Special Categories of Personal Data through the Service. The Data Processor shall not be liable for the processing of such data uploaded in violation of the Agreement and these Terms and Conditions.

3. DATA PROCESSOR'S RESPONSIBILITIES

3.1. Confidentiality: The Data Processor undertakes to maintain the confidentiality of Personal Data. This confidentiality obligation shall survive termination of the Agreement.

3.2. Security: The Data Processor implements and maintains appropriate technical and organizational security measures designed to protect Personal Data from Data Leakage. These measures include, but are not limited to:

Encryption: Encryption of transmitted data using modern protocols (TLS 1.2+) and encryption of data at rest.

Access Control: Implementation of the principle of least privilege, strict control of employee access to Personal Data based on a need-to-know basis, and multi-factor authentication.

Network Security: Firewalls, intrusion detection and prevention systems, and regular vulnerability scanning.

Physical Security: Protection of physical servers in Tier III+ data centers in the UAE with 24/7 access control, video surveillance, and fire protection systems. Security Policies: Internal information security policies and procedures for employees that must be followed.

Risk Assessment: Regularly conduct data security risk assessments.

3.3. Subprocessing: The Data Processor has a general right to engage other processors ("Subprocessors") to provide services. The Data Processor will enter into written contracts with all Subprocessors that contain data protection obligations no less stringent than those set out in this Policy. A current list of approved Subprocessors (including hosting providers, such as the AWS Middle East (UAE) Region) is published at [link to the Subprocessor page] and may be updated from time to time. The Data Processor will notify the Data Controller of any planned changes regarding the addition or replacement of a Subprocessor. If the Data Controller has a reasonable objection to such a change, it must notify the Data Processor within 10 (ten) days of the notice. In the event of a justified objection, the Data Processor will use reasonable efforts to offer an alternative solution. If such a solution is not found, the Data Controller has the right to terminate the Agreement.

3.4. Assistance to the Data Controller: The Data Processor undertakes to provide the Data Controller with the necessary assistance to ensure the latter's compliance with the requirements of the PDPL, in particular:

Rights of Data Subjects: The Data Processor provides the Data Controller with the technical capability to fulfill requests from Data Subjects for access, correction, deletion, and portability of data within the Personal Account functionality. If the request is received directly by the Data Processor, the latter will forward it to the Data Controller within three (3) business days.

Impact Assessments: The Data Processor provides the Data Controller with the available information necessary to conduct a Data Protection Impact Assessment (DPIA), if required.

Consultations with the Regulator: The Data Processor will assist the Data Controller in consultations with the UAE Data Protection Authority, if necessary.

4. DATA BREACH NOTIFICATION

4.1. Detection: The Data Processor will notify the Data Controller promptly upon detection of a Data Breach, without undue delay, and in any event no later than 36 (thirty-six) hours after becoming aware of the Breach.

4.2. Contents of Notification: The Notification will contain at least the following information:

A description of the nature of the Data Breach, including the categories and approximate number of Data Subjects and records affected.

The anticipated impact of the Data Breach.

The measures taken by the Data Processor to address the Breach and mitigate its potential negative impact.

Contact details of the Data Protection Officer or other representative for further information.

4.3. Cooperation: The Data Processor will take all reasonable steps to assist the Data Controller in investigating the incident, fulfilling the obligation to notify the UAE Data Protection Authority within 72 hours and the affected Data Subjects (if required by law), and minimizing any potential damage.

5. INTERNATIONAL DATA TRANSFERS

5.1. The Data Processor will process and store Personal Data exclusively in the United Arab Emirates, unless otherwise required to provide services to a specific Data Controller (e.g., if the Data Controller has explicitly selected a storage region outside the UAE in the Service settings).

5.2. Any international data transfer outside the UAE will be carried out by the Data Processor only if an adequate level of protection is ensured as required by the PDPL, for example by:

Obtaining the explicit consent of the Data Controller and, where applicable, the data subject.

Implementing binding corporate rules or standard contractual clauses that ensure a level of protection consistent with the PDPL requirements. Transfers to jurisdictions recognized by the Executive Council of the UAE Data Protection Authority as providing an adequate level of protection.

6. DELETION OR RETURN OF DATA

Upon completion of services related to the processing of Personal Data, at the Data Controller's discretion and in accordance with the settings in the Personal Account, the Data Processor will delete or return all Personal Data and delete existing copies thereof, unless UAE law requires the Data Processor to retain such data. This obligation does not apply to data that the Data Processor is required to retain under applicable UAE law, nor to anonymized aggregated data used for analytics.

7. AUDITS

7.1. The Data Processor shall provide all necessary information to demonstrate compliance with the obligations set out in this Policy and the PDPL.

7.2. The Data Processor authorizes the Data Controller or an appointed independent auditor who is not a competitor of the Data Processor to conduct audits (no more than once a year) to verify compliance with this Policy. The audit must be agreed upon in advance (at least 30 days in advance), conducted during the Data Processor's working hours, with minimal interference with its activities, and maintained in strict confidentiality. All audit costs shall be borne by the Data Controller.

8. FINAL PROVISIONS

8.1. This Policy is governed by the laws of the United Arab Emirates.

8.2. Any disputes arising from this Policy shall be resolved in the courts of the Emirate of Dubai, UAE, as specified in the Agreement.

8.3. In the event of a conflict between the terms of this Policy and the terms of the Agreement, the terms of this Policy shall prevail with respect to personal data processing.

CONTACT INFORMATION FOR NOTICES RELATED TO THIS POLICY:

BOTTO PLATFORM - FZCO

Address: Dubai Silicon Oasis, DDP, Building A1, Dubai, United Arab Emirates

Attn: Data Protection Officer

Email: privacy@botto.ai