AGREEMENT ON THE PROCESSING OF PERSONAL INFORMATION

This Agreement on the Processing of Personal Information has been stipulated between **Userbot S.r.l. [*LLC*]**, with registered office at Via Vincenzo Monti 79/2, Milano (MI), tax ID number and IVA [*Value-Added Tax*] code 10017690966, in its role as Data Supervisor (below referred to as "**Userbot**" or "**Supervisor**" for brevity) and the party defined in the "Terms and Conditions" as **User**, in its role as Data Controller (below referred to as "**User**" or "**Controller**").

This Agreement on information processing is an essential part of the "Terms and Conditions" accepted by the User.

The contractual parties can be referred to collectively as "**Parties**" and individually as "**Party**".

Given that:

(i) Userbot is a *start-up* company operating in the field of Artificial Intelligence and generally in the development, production, and sale of technological products and/or services;

(ii) With the User's acceptance of the Terms and Conditions, the Parties finalize the contract (below referred to as "**Contract**"), with which Userbot commits to provide a chatbot service with use of Artificial Intelligence, for the User's Website, page, or platform (below referred to as "**Services**");

(iii) In order to provide the Services, Userbot will process some personal information for which the User is the controller;

(iv) Prior to authorizing Userbot to provide the Services, the Controller has assessed whether Userbot can offer sufficient guarantees to set technical measures in place for ensuring adequate protection of the processed information and the rights of the concerned parties;

(v) With this agreement (below referred to as "**Agreement**"), the User intends to appoint Userbot as Data Supervisor for which he/she is the Controller and provide it with the necessary information for processing.

Given what was stated above, the Parties agree and stipulate what follows.

1. Definitions

In regard to this agreement, the definitions included in the Contract, whenever relevant, and the definitions listed below are hereby applicable:

- **"Personal Information"** refers to all the information related to an identified or identifiable physical person (below referred to as **"Concerned Party"**) that the Data Supervisor processes on behalf of the Controller in order to provide the Services;

- **"Protection Authority"** refers to the personal information protection authority established by Law no. 675 dated December, 31, 1996;

- **"Applicable Law"** refers to EU Regulation 2016/679 issued by the European Parliament and Council on April 27, 2016, in relation to the protection of physical people and the processing of their personal information and to the free circulation of said information (below referred to as "**Regulation**"), and to D.Lgs. [*Legislative Decree*] 196/2003 and subsequent modifications and any other laws or decrees in the matter of personal information protection applicable in Italy, including the measures taken by the Protection Authority;

- The term **"Technical and Organizational Security Measures"** refers to the measures provided for by article 32 of the Regulation, which in any case, have to exceed those described in articles 31, 33, and subsequent ones of D.Lgs. [*Legislative* Decree] 196/2003 and in the related Attachment B), and by the decisions made by the Protection Authority; the aforementioned articles of D.Lgs. 193/2003 and the related decisions made by the Protection Authority are invoked in this document because of their material relevance, regardless of the validity of said regulations at a national level.

2. Appointments

By signing this Agreement, the Data Controller grants to Userbot, who accepts, the title of Data Supervisor, in compliance with article 28 of the Regulation.

3. Duration

The Agreement will become effective on the date of signing and will remain valid until Contract termination, regardless of the reason for said termination or until the end date for personal information processing if, for any reason, it is subsequent to the Contract termination date.

4. Information Processing Activities

4.1. This Agreement refers to all processing activities connected to the provision of Services (below referred to as "**Processing Activities**").

4.2. Processing activities will be functional to the Services being offered and to all the additional activities that the Data Controller might require from the Data Supervisor to provide the aforementioned Services.

5. Types of Personal Information and Categories of Concerned Parties

5.1. Information Processing Activities will mostly include common personal information. In the event that, in order to perform said actions, the Supervisor must also process personal information belonging to special categories, the Data Controller is responsible to acknowledge the situation to the Supervisor, in compliance with the methods described in the "Privacy Policy" section of the "Terms and Conditions".

5.2. The Supervisor will process Personal Information related to the users of the website, page, or platform owned by the User.

6. Obligations of the Supervisor

The Supervisor makes the commitment to the Controller to comply with the following obligations, in addition to any other obligations provided for by applicable laws:

a. process Personal Information in full compliance with the principles and regulations provided for by current privacy laws and exclusively for the purpose of providing the Services indicated in this Agreement as well as for any other reasons that the Controller might indicate in the future;

b. process Personal Information in compliance with the instructions provided by the Controller, with the instructions included in the Contract or with any other instructions that the Controller might decide to add to improve the efficiency of the procedures; any additional instructions provided by the Controller will be notified to the Supervisor in writing or transmitted to the Supervisor by certified email;

c. ensure that all individuals authorized to process personal information comply, upon committing in writing, with the full confidentiality of said information and that, for that purpose, they comply with the instructions provided by the Supervisor and, in any case, under its constant supervision;

d. do not disclose to third parties and in general, do not divulge the received information, if not in the presence of specific conditions granting additional actions;

e. keep Personal Information separate from the information processed on behalf of other subjects, based on logic security criteria, and ensure that every copy of stored Personal Information – including copies held by employees, subcontractors, agents and associates – is permanently destroyed or returned when it becomes no longer necessary for the Processing Procedures, in compliance with the measures provided for by applicable laws. It remains understood that the Controller will be obligated to once again provide the Supervisor with any information that was destroyed or returned and that the Supervisor might need to defend its legal rights in a third-party dispute related to the execution of the contract;

f. adopt suitable measures to address security violations that resulted, whether accidently or maliciously, in the destruction, loss, modification, unauthorized distribution, or access to Personal Information, and in any case, fully cooperate with the Controller to eliminate or at least minimize the impact of these events;

g. notify the Controller, without any unjustified delay, of every possible event that could qualify as *data breach*, in compliance with applicable laws, and promptly inform the Controller about any further event, fact, or circumstance, whether foreseeable or not, that might result in an elevated risk to the rights and freedom of the parties involved in the processing activities;

h. assist the Controller, limited to the processing of Personal Information, in ensuring compliance with personal information security measures. Specifically: (i) with the notification of personal information violations to the Protection Authority or to other competent monitoring authorities, and also to the concerned parties if their rights and freedom are put at risk; (ii) if necessary, with a suitable assessment of the impact on data

protection and with preventive consultation procedures with the Protection Authority or other competent authorities;

i. if the conditions exist, create and maintain, whether digitally or on paper, a register of all information processing activities related to the implementation of the Agreement, specifically including: (i) contact information, in addition to the contact information of the Controller and the data protection supervisor; (iii) if necessary, the details related to any transfer of information received outside the European Economic Area, with the indication of the third-party country or organization where the information was transmitted as well as the reason for the transmission of said information and the implemented measures to protect it; (iv) a general description of the technical and organizational measures adopted to ensure data protection.

j. provide, within the limits of competence, the highest cooperation to the Controller, in the case of petitions submitted by the Concerned Parties and received by the Supervisor;

k. notify the Controller if the received instructions entail a violation of applicable laws;

l. assist the Controller in fulfilling any requests sent by the Protection Authority or any other competent authorities, or any procedures or inspections initiated against the Controller, by immediately executing the received instructions and providing copies of any requested documentation;

m. designate in writing individuals to appoint as administrators of the systems used for data processing, specifically indicating the areas of competence based on the assigned authorization profiles and reporting the list of system administrators in a document to be updated and made available in case of inspections, including by the Protection Authority. In compliance with the Measure issued on 11/27/2008 by the Protection Authority and titled "Controller's Measures and Precautions for Information Processed Electronically in Relation to the Appointment of a System Administrator" and subsequent modifications, the Data Supervisor must evaluate the subjective characteristics necessary for the appointment and directly and specifically store the identification information of the individuals selected as system administrators; the Supervisor will also have to set up systems suitable for the registration and related preservation of the logical accesses (electronic authentication) created by the system administrators for data elaboration systems and electronic archives.

7. Information Security

The Supervisor commits to adopt all the preventive technical and organizational security measures designed to ensure an adequate security level in relation to Personal Information, that are deemed adequate to minimize the risk of destruction, loss, modification, unauthorized distribution, or access, whether accidental or malicious, to the received information. Specifically, the Supervisor also commits to comply with and implement all the Technical and Organizational Security Measures, in addition to any other measures that the Controller might request in relation to specific information processing actions.

8. Sub-Suppliers

8.1. The Supervisor is authorized to use additional suppliers in order to provide the Services. Said sub-suppliers will process the User's personal information as data supervisors, authorized by an information processing agreement stipulated with the User or by an agreement stipulated between the sub-suppliers and the Supervisor, in compliance with article 28, paragraph 4 of the Regulation, that will appoint said sub-suppliers as additional supervisors on behalf of the Controller, binding them to the same personal information protection obligations applied to the Supervisor by virtue of this agreement and current laws.
Specifically, the sub-supplier will have to provide adequate guarantees in regard to the implementation of adequate technical and organizational security measures, so to comply with the requirements imposed by Applicable Laws. It is understood that, if the sub-supplier fails to comply with its information protection obligations, the Supervisor will still be fully liable for the sub-supplier failed obligations towards the Controller.

8.2. The Supervisor will have to inform the Controller about any modification intention related to the addition, replacement or removal of other supervisors, as provided for by article 8.1, therefore giving the Controller an opportunity to object to said modifications.

9. Transfer of Personal Information

9.1. In the event that, in order to provide the Services, the Supervisor uses sub-suppliers located in countries outside the European Economic Area, the transfer of Personal Information will take place based on an agreement stipulated between the User, as exporting Data Controller, and the sub-supplier receiving the Personal Information, as importer, in compliance with article 46 of the Regulation. Said agreement will be drafted based on the sample clauses provided for by Decision 2010/87/EU issued by the European Commission or on other sample clauses provided for by the Commission in compliance with the Regulation, it being understood that the Supervisor will be responsible for the sub-suppliers signing the aforementioned clauses.
9.2. Effective now, the Controller grants to Userbot a specific mandate to jointly sign said sample clauses with the sub-supplier, in the name and on behalf of the User.

10. Audit

The Supervisor commits to provide to the Controller, upon request, all documentation and reports attesting its compliance with the required obligations, pursuant to this Agreement, with particular attention to the security measures that have been adopted.

The User

_____

Userbot S.r.l. [*LLC*]

_____

Please send this properly signed Appointment Act to email address amministrazione@userbot.ai, including First and Last Name of the Controller (if physical person) or Company Name (if legal entity) in the body of the email.