DATA PRIVACY AGREEMENT

CALELLA, 02/07/2024

PARTIES:

On the one hand, Gerard Cano Palau (SocialGency Tech), as the Data Controller, with Tax ID (NIF) 77633720A and registered office at Francesc Saula i Pujals n.16 - 08370 Calella (Barcelona), hereinafter referred to as the CONTROLLER.

And on the other hand, Noor Mohammad, as the Data Processor, with passport number A13110768, and registered office at Middle Paikepara Mirpur Mirpur, 1216 Dhaka, hereinafter referred to as the PROCESSOR.

Both parties mutually acknowledge their legal capacity to enter into this data processing agreement and

DECLARE:

1. Both parties will process the personal data subject to this agreement in accordance with the provisions of the Regulation (EU) 2016/679 of April 27, 2016 (GDPR) and the Organic Law 3/2018 of December 5 (LOPDGDD).

2. The CONTROLLER has contracted the services of the PROCESSOR, which consist of: Services provided: Development of AI-powered chatbots and other software development and maintenance.

Duration of the contract: linked to the duration established in the aforementioned service contract code SG-2024-P2.

3. To fulfill these services, the PROCESSOR needs access to and processing of personal data, which is the responsibility of the CONTROLLER.

4. In compliance with Article 28 of the GDPR, the PROCESSOR provides sufficient guarantees to implement appropriate technical and organizational policies to apply the security measures established by current regulations and protect the rights of data subjects.

Therefore, both parties agree to enter into this agreement with the following

DATA PROCESSING INSTRUCTIONS:

1. Purpose, Nature, and Scope of the Processing:

- Purpose of the processing: Development of AI-powered chatbots for different phone lines through WhatsApp.

- Obligation to inform the data subject about the processing: this will be exclusively the responsibility of the CONTROLLER.

- Location of the processing: remote access to the CONTROLLER's systems. The PROCESSOR is not authorized to incorporate the data into its systems.

2. Types of Personal Data and Categories of Data Subjects:

- Types of personal data to which the PROCESSOR will have access: ID/Passport number, Full name, Postal or email address, Telephone number.

- Other types of data: Commercial information.

- Categories of data subjects: Clients and users, Contact persons, Applicants.

- Authorized processing operations: strictly necessary to achieve the purpose of the processing.

3. Obligations and Rights of the CONTROLLER:

- The CONTROLLER guarantees that the data provided to the PROCESSOR have been obtained legally and are adequate, relevant, and limited to the purposes of the processing.

- The CONTROLLER will provide the PROCESSOR with all necessary information to carry out the tasks subject to the processing.

- The CONTROLLER warns the PROCESSOR that if it determines on its own the purposes and means of the processing, it will be considered a data controller and will be subject to complying with the applicable provisions of current regulations.

4. Obligations and Rights of the PROCESSOR:

- The PROCESSOR undertakes to respect all obligations that may correspond to it as a data processor in accordance with current regulations and any other applicable provision or regulation.

- The PROCESSOR is prohibited from using the data it has access to for any purpose other than the processing or in breach of this agreement.

- The PROCESSOR must provide the CONTROLLER with the necessary information to demonstrate compliance with the agreement and allow necessary inspections and audits to evaluate the processing.

5. Authorized Personnel for Processing:

- The PROCESSOR guarantees that the personnel authorized to process the data has committed expressly and in writing to confidentiality or is subject to a legal obligation of confidentiality.

- The PROCESSOR must take measures to ensure that any person acting under its authority and having access to personal data can only process them in accordance with the CONTROLLER's instructions or if legally required.

- The PROCESSOR guarantees that the authorized personnel has received the necessary training to ensure that the protection of personal data is not at risk.

6. Security Measures:

- The PROCESSOR acknowledges its awareness of the obligations arising from data protection regulations, especially regarding the implementation of security measures for the different categories of data and processing as established in Article 32 of the GDPR.

- The PROCESSOR guarantees that these security measures will be adequately implemented and will assist the CONTROLLER in complying with the obligations established in Articles 32 to 36 of the GDPR, considering the nature of the processing and the information available to the PROCESSOR.

- The CONTROLLER must conduct a risk analysis of the processing to determine the appropriate security measures to ensure the security of the processed information and the rights of data subjects. If risks are identified, the CONTROLLER must provide the PROCESSOR with an impact assessment report for implementing appropriate measures to avoid or mitigate them.

- The PROCESSOR must analyze any potential risks and other circumstances affecting the security attributed to it. If any risks are identified, the PROCESSOR must inform the CONTROLLER to evaluate the impact.

7. Security Breach:

- Any security breaches discovered by the PROCESSOR must be notified without undue delay to the CONTROLLER to allow for the necessary measures to remedy and mitigate the effects. Notification is not required if the breach is unlikely to pose a risk to the rights and freedoms of natural persons.

- The notification of a security breach must contain, at a minimum, the following information:

  - Description of the nature of the breach.
  - Categories and approximate number of affected data subjects.
  - Categories and approximate number of affected data records.
  - Possible consequences.
  - Measures taken or proposed to remedy or mitigate the effects.
  - Contact details for more information (DPO, security officer, etc.).

8. Communication of Data to Third Parties:

- The PROCESSOR cannot communicate the data to third-party recipients unless it has obtained prior written authorization from the CONTROLLER. Any such authorization must be annexed to this agreement.

- Data transfers to public authorities in the exercise of their public functions do not require authorization from the CONTROLLER if such transfers are necessary to achieve the purpose of the processing.

9. International Data Transfers:

- The PROCESSOR cannot transfer data to third countries or international organizations outside the EEA unless it has obtained prior written authorization from the CONTROLLER. Any such authorization must be annexed to this agreement.

10. Subcontracting Data Processing:

- The PROCESSOR is prohibited from subcontracting any third party to carry out any data processing assigned by the CONTROLLER unless it has obtained prior written authorization. Any such authorization must be annexed to this agreement.

11. Rights of Data Subjects:

- The PROCESSOR must create, whenever possible and considering the nature of the processing, the necessary technical and organizational conditions to assist the CONTROLLER in fulfilling the obligation to respond to data subject rights requests.

- If the PROCESSOR receives a request to exercise these rights, it must immediately notify the CONTROLLER, no later than the next business day after receiving the request, along with any other relevant information to resolve it.

12. Liability:

- In accordance with Article 82 of the GDPR, the CONTROLLER shall be liable for damages caused in any processing operation in which it participates and fails to comply with the GDPR. The PROCESSOR shall only be liable for damages caused by the processing if it has failed to comply with GDPR obligations specifically addressed to the PROCESSOR or has acted outside or against the lawful instructions of the CONTROLLER. The PROCESSOR is exempt from liability if it can prove that it is not responsible in any way for the event that caused the damage.

13. End of Service Provision:

- Once the service provision subject to this agreement is completed, if the PROCESSOR has stored personal data or any other document and/or medium provided by any means, it must return, delete, or deliver them to a new processor according to the CONTROLLER's decision, including any existing copies. The PROCESSOR must issue a certificate of return or destruction if required by the CONTROLLER.

- Data should not be deleted if a legal provision requires their retention, in which case the PROCESSOR must keep them, blocking and limiting their processing while responsibilities from its relationship with the CONTROLLER may arise.

- The PROCESSOR must maintain the duty of secrecy and confidentiality of the data even after the relationship subject to this agreement has concluded.

In witness whereof, both parties sign this agreement, in duplicate, in the place and on the date indicated above.

Noor Mohammad
28/07/2024

_____	_____
CONTROLLER	PROCESSOR