D A T A P R O C E S S I N G A G R E E M E N T

For Certainly Group ApS' processing of Data

Data Processing Agreement for

Certainly Group ApS's Processing of Data

WHEREAS a services agreement has been entered into

between

you as the customer
(the "**Controller**" as listed in **Annex A**)

and

Certainly Group ApS
(the "**Processor**" as listed in **Annex A**)

(referred to individually as a "**Party**" or collectively as the "**Parties**")

(the "**Services Agreement**")

for the Processor's performance of services;

WHEREAS the Processor in their performance of the services will be processing personal data on behalf of the Controller;

NOW THEREFORE the Parties have entered into this Data Processing Agreement ("**DPA**") for the purposes of adherence to Article 28(3) of Regulation 2016/679 (the GDPR) and to ensure the protection of the rights of the data subjects.

1. INSTRUCTIONS ON DATA PROCESSING

1.1 Subject to this DPA, the Processor processes on behalf of and on the instruction of the Controller the categories of personal data stated in sections 2.3, for the purposes stated in section 2.5, for the activities stated in section 2.6 and conduct the types of processing stated in section 2.7.

1.2 The Processor may process personal data without the explicit consent of the Controller if required under EU law and/or Danish law. The Processor informs the Controller hereof before the processing occurs, unless prohibited by law.

1.3 The Processor may not process personal data for its own purposes. The Processor ensures that access to personal data is limited to only employees who need to access the data for the purpose of carrying out the duties they are tasked with.

2. PERSONAL DATA AND DATA PROCESSING

2.1 The DPA forms part of the Services Agreement entered into between the Controller and the Processor. As part of the Processor's performance of the agreement, the Processor processes on behalf of the Controller personal data concerning the Controller's employees and customers ("**Data Subjects**").

2.2 "Personal data" means any information relating to an identified or identifiable natural person, in accordance with art. 4(1) of regulation (EU) 2016/679 of 27 April 2016 ("**General Data Protection Regulation**").

2.3 The Processor processes the following categories of personal data on Data Subjects:

a. Name and phone number
b. E-mail address and registered address
c. Job title
d. User behavioral data (page views, clicks, field changes, form submissions, chatbot usage statistics, session and conversations ID.
e. User intent and Queries. General types of inquiries users are asking about, categorized into common areas such as product inquiries, support issues, or feedback.
f. Any other personal data that the data exporter transfers to the data importer.

2.4 The Processor does not process personal social security/identification numbers or special categories of personal data about Data Subjects, cf. art. 9 and 10 of the General Data Protection Regulation.

2.5 The Processor processes personal data for the Controller with the following purposes:

1. Handling the conversation chat on behalf of the Controller.
2. Improving chatbot performance
3. Insights and analytics for Controller
4. Sending an order confirmation;
5. Assessing the needs of business to determine suitable products and solutions;
6. Sending requested product or service information;
7. Sending product updates or warranty information;
8. Responding to customer service requests;
9. Invoicing and managing payments;
10. Engaging Partners to provide necessary services on our behalf;
11. Using 3rd party service providers to host our cloud-based services
12. Sending marketing communications;

2.6 The Processor's processing of personal data for the Controller includes the following activities:

1. Storage of Personal Data
2. Transfer of personal data to third-party providers whom the Controller has chosen to connect to
3. Reception of personal data from third-party providers whom the Controller has chosen to connect to

2.7 Types of processing performed by the Processor include the following:

Collection, storage, organization, internal sharing, erasure and any other form of processing that is necessary to achieve the purpose of the processing

3. STORAGE OF DATA

3.1 Personal data is stored on behalf of the Processor on servers at the Processor's sub-processors in the EU.

3.2 By their signature to this DPA, the Controller approves by way of explicit consent to the transfer of personal data to the USA for storage purposes. The Processor is liable to procure the legal foundation of the transfer of personal data prior to the transfer taking place.

3.3 The Processor is obliged to inform the Controller in writing if the Processor finds an instruction of the Controller to be in violation of the General Data Protection Regulation or other data protection legislation in EU law or member state law.

3.4 The Processor must inform the Controller of any change of supplier of server hosting prior to the change and give the Controller the option to object.

4. PROCESSOR'S OBLIGATIONS

4.1 The Processor trains and instructs employees in confidential processing of personal data and ensures that processing is done solely in accordance with the purposes of the DPA and the Controller's instructions. The Processor ensures that their employees have committed themselves to confidentiality with respect to all personal data and treat personal data accordingly.

4.2 The Processor processes personal data only on instruction from the Controller and only in accordance with the instructions as well as any other purposes agreed between the Parties in writing. The processing of personal data shall be performed in accordance with good data processing practices.

4.3 The Processor is obliged to store personal data on behalf of the Controller and in accordance with its instructions throughout the duration of the Services Agreement between the Parties unless the Controller instructs the Processor to store the personal data for a longer period.

4.4 At the expiry/termination of the Services Agreement and at the Controller's behest, the Processor shall 1) erase or 2) return to the Controller all personal data and remove existing copies. The Processor shall erase personal data from all IT systems when so instructed by the Controller and future storage no longer serves a legitimate purpose.

4.5 The Processor has the duty to establish, implement and maintain, organizational, administrative and IT technical security measures that prevent personal data from accidentally or illegally being destroyed or lost, deteriorate or be disclosed to unauthorized persons, abused or otherwise processed in violation of the law. The Processor shall give instructions that place responsibility for, and describe processing and erasure of, personal data and operation of IT equipment. At the Controller's request, the Processor shall provide the Controller with information adequate to check whether the mentioned technical and organizational security measures are implemented.

4.6 The Processor shall, to the extent possible, assist the Controller by appropriate technical and organizational measures in complying with the Controller's obligation to respond to Data

Subjects' exercise of their rights in accordance with chapter 3 of the General Data Protection Regulation. The Controller is responsible for direct communication with the Data Subjects. The Controller shall put its request for the Processor's assistance in writing and endeavor to describe as accurately and limited as possible the activities with which the Controller is requesting the Processor's assistance.

4.7 In order to assist the Controller in its fulfilment of its obligation to respond to requests for exercising the Data Subject's rights laid down in chapter 3, the Processor has implemented the following technical and organizational measures:

The request shall be submitted to the Processor's contact person as stipulated in Annex A. As soon as a request has been submitted, the Processor's contact person will instruct its Data Protection Officer to comply with the request. By using the Processor's IT system, the Processor's Data protection Officer (DPO) will in cooperation with other staff appointed by the DPO take the necessary steps to ensure the compliance with the request by the nature of what has been requested given the right(s) exercised by the Data Subject. To comply with and respond to such request, the Processor will employ SOC type I and Type II security standards as technical measures, along with other measures that may be relevant or necessary for the compliance with the request. The Controller and its staff are entitled to be physically present at the Processor's offices and facilitate and inspect the compliance with the request.

4.8 Upon the written request by the Controller to the Processor, giving not less than thirty (30) days' notice, the Controller is entitled to audit the Processor's compliance of this DPA, once a year, at the Processor's its own costs, by accessing the technical and organizational security measures of the Processor in accordance with applicable data protection law. Such audit shall be carried out by the Controller or an inspection authority appointed by the Controller composed of independent persons in possession of the required professional qualifications bound by a duty of confidentiality. The Controller will furnish immediately after the verification or inspection to the Processor a copy of the report of a such audit. The Processor shall cooperate with such audit or inspection. If an audit or inspection shows that the Processor does not take and implement appropriate technical and organizational security measures in accordance with applicable data protection law, the Processor and the Controller shall discuss and agree to improve the technical or organizational security measures in good cooperation.

5. THE CONTROLLER'S OBLIGATIONS

5.1 The Controller warrants that the processing of personal data in accordance with the Controller' instructions is legal.

5.2 The Controller must exercise good data processing practices, including securing equipment and infrastructure in such a way that it does not pose a risk to the Processor's compliance with its obligations. This applies for example to the securing of the Controller's network, endpoint protection of devices with antivirus and firewalls, structured and secure handling of user accounts and access, securing of backup and testing of the ability to recover data.

5.3 The Controller shall make reasonable efforts to ensure that any third-party tools that the Controller connects to its software platform are GDPR compliant. The Controller shall make

reasonable efforts to apply the obligations in sections 5.1 and 5.2 of this Data Processing Agreement to the Controller's use of third-party tools in connection to its software platform.

6. MUTUAL REPORTING OBLIGATIONS

6.1 The Processor shall forward to the Controller any third-party inquiries regarding the content of data originating from the Controller's systems or Data Subjects.

6.2 The Controller shall forward to the Processor inquiries and information relating to the Processor's specific processing of data. The Processor must inform the Controller of any deviations from the given instructions regarding the processing. In particular, deviations able to compromise data accuracy must be reported.

6.3 If there is any suspicion, or an incident indicating, that a personal data breach has occurred it shall be immediately reported to the other Party.

6.4 In case a personal data breach has occurred, the Processor shall immediately notify the Controller who in turn notifies the Danish Data Protection Agency (Datatilsynet) of the breach within 72 hours of the Processor having been notified of the breach, unless it is unlikely that the personal data breach endangers the Data Subjects' rights or rights of freedoms.

7. SUB-PROCESSING

7.1 The Processor is authorized to use sub-processors without further written permission from the Controller. The Processor shall notify the Controller in writing of the identity of new sub-processors before entering into an agreement with the respective sub-processors, allowing the Controller to object to the appointment of the sub-processor in question. A list of the Processor's sub-processors as at the date of the formation of this DPA is attached as **Annex B.**

7.2 The Processor shall notify the Controller in writing of any planned major additions or replacements of sub-processors no later than one (1) month prior to the changes taking effect.

7.3 Having received notice, the Controller has the right to make legitimate objections to the appointment of the new sub-processor. In that case, giving one (1) months' notice, the Processor is entitled to terminate all agreements with the Controller, according to which the Processor processes personal data for the Controller.

7.4 Prior to letting the sub-processor commence processing personal data, the Processor shall enter into a written agreement with the sub-processor, as a minimum making the sub-processor subject to the obligations which the Processor is subject to under the DPA, including the obligation to implement adequate technical and organizational measures to ensure that the requirements of the General Data Protection Regulation be satisfied.

8. INTERNATIONAL TRANSFERS

8.1 Any transfer of data to a third country or an international organization by the Processor shall be done only based on documented instructions from the Controller or to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of the General Data Protection Regulation.

8.2 The Controller agrees that where the Processor engages a sub-processor in accordance with Clause 7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of the General Data Protection Regulation, the Processor and the sub-processor can ensure compliance with Chapter V of the General Data Protection Regulation by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of the General Data Protection Regulation, provided the conditions for the use of those standard contractual clauses are met.

9. AUTOMATIC DATA DELETION

9.1 Customer data, including personal information and files, will be scheduled for deletion from the Certainly Group ApS infrastructure after 3 months of inactivity on the platform. Customers can choose to have their data deleted with a shorter notice period. This can be done from the platform administration interface.

10. NON-COMPLIANCE AND TERMINATION

10.1 Without prejudice to any provisions of the General Data Protection Regulation and/or Regulation (EU) 2018/1725, in the event that the Processor is in breach of its obligations under this DPA, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with the DPA or the DPA is terminated. The Processor shall promptly inform the Controller if for whatever reason it is unable to comply with this DPA.

10.2 The Controller shall be entitled to terminate the DPA insofar as it concerns processing of personal data in accordance with this DPA if:

(1) the processing of personal data by the Processor has been suspended by the Controller and if compliance with the DPA is not restored within a reasonable time and in any event within one (1) month following suspension;
(2) the Processor is in breach of the DPA or its obligations under the General Data Protection Regulation and/or Regulation (EU) 2018/1725;
(3) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to the DPA or to the General Data Protection Regulation and/or Regulation (EU) 2018/1725.

10.3 The Processor shall be entitled to terminate the DPA insofar as it concerns processing of personal data under the DPA where, after having informed the Controller that its instructions infringe applicable legal obligations pursuant to this DPA, the Controller unreasonably insists on compliance with the instructions.

10.4 Following termination of the DPA, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with this DPA.

10.5 The Controller is entitled to terminate the Services Agreement if by the suspension of the processing of personal data or termination of this DPA the Processor's performance of its obligations under the Services Agreement becomes impossible or severely impeded due to

the Processor's inability to process personal data on behalf of the Controller without the Controller being in non-compliance with the General Data Protection Regulation or Regulation (EU) 2018/1725.

11. DURATION

11.1 The DPA will enter into force by signing and shall remain in force until the Services Agreement is terminated by either Party or the business relationship terminates.

12. CHOICE OF LAW AND LEGAL VENUE

12.1 This DPA shall be governed by and construed in accordance with the laws of Denmark, without giving effect to any choice of law or conflict of law provisions.

12.2 The courts of Denmark have sole jurisdiction to hear any claim in any matter brought under this Agreement, including claims brought in tort/common law, or similar, or equity, in matters relating to this Agreement.

.o0o.

APPENDIX

TO DATA PROCESSING AGREEMENT

Annex A

LIST OF PARTIES

Controller:

1. Name: [ ]

Address:
[street and No.]
[post code and city]
[country]

Company reg. No.: [ ]

Contact person's name, position and contact details:

[name], [position], # [phone number], email: [ ]

Signature and date:

On behalf of the **Controller**:

_____

[name]

[position]

Role (controller/processor): **Controller**

Processor:

1. Name: Certainly Group ApS

Address:
Kronprinsessegade
8, 3.,
Copenhagen 1306
K, Denmark

Company reg. No.: 42292540

Contact person's name, position and contact details:

Hans Peter vith, COO, email: hpv@certainly.io

Signature and date:

On behalf of the **Processor**:

_____

Annex B

List of Sub-processors

Vendor	Security standards
Amazon AWS - eu-west-1 (Ireland)	https://aws.amazon.com/security
Microsoft Corporation - Ireland	https://azure.microsoft.com/en-us/explore/trusted-cloud/privacy/
Nuclia - EU (Spain)	https://nuclia.com/privacy-security/
UBI - Singapore	https://chat.uib.ai/privacy
Seidor - EU (Spain)	https://www.seidor.com/ca-es/avis-legal-i-politica-de-privacitat
OpenAI - USA	https://openai.com/enterprise-privacy/