Data Processing Agreement

This Data Processing Agreement forms part of the Contract for Services

BETWEEN:	CC4ALL B.V. KVK No.: 65298861 Lange Dreef 15 4131NJ Vianen The Netherlands Email: info@contactcenter4all.com (the "Data Processor")
AND	Each individual ContactCenter4ALL Customer that ContactCenter4ALL processes data for and that has not otherwise entered into a valid data processor agreement with ContactCenter4ALL (the "Data Controller") (hereinafter referred to individually as a "Party" or together as the "Parties")

1. Introduction

This Data Processing Agreement ("DPA") specifies the Parties data protection obligations, which arise from the Data Processor's processing of personal data on behalf of the Data Controller under the quote, service agreement or other agreement between the Parties ("the Agreement").

The DPA is adopted as an appendix to the Agreement. If any provision of this DPA is inconsistent with any term(s) of the Agreement, the DPA will prevail.

2. Purpose, scope and responsibillities

2.1 The Data Processor shall only process personal data in accordance with the terms of this DPA.

2.2 The Data Processor shall process personal data for the limited purpose of performing the obligations set out under the Agreement. Data may, for that purpose, be processed by any of the Data Processor's entities.

2.3 Data processing by the Data Processor shall include such actions as may be specified in the Agreement.

2.4 The term of this DPA shall continue until the latter of the following: the termination of the Agreement, or the date at which the Data Processor ceases to process personal data for the Data Controller.

2.5 The personal data to be processed by the Supplier concerns the categories of data, the categories of data subjects and the purposes of the processing set out in **Appendix 1.**

2.6 With the exception of the data described in **Appendix 1**, in no event will the data processed by the Data Processor include (examples are not exhaustive):

a) Personal data as set out in art. 9 or 10 in Regulation 2016/679 of 27 April 2016
b) Financial data,
c) Personal data regarding criminal offenses, or
d) Data regarding persons' economy, taxes, debt, sick days, family relations, residential circumstances, car, personality tests, exams, or CVs.

3. CC4ALL Services

3.1. The Agreement enables the Data Controller to install and use the software developed by the Data Processor:
CC4Cloud, CC4Skype, CC4Teams, CC4Dynamics, CC4ServiceNow and additional supported integrated services (hereinafter referred to as a "CC4ALL Services").

The CC4ALL Services enables the Data Controller's employees (with by the Data Controller assigned access rights) to handle customer contact without the Data Processors' participation or knowledge.

3.2. The Data Processor undertakes no responsibility for data accessed by the Data Controller in the CC4ALL Services.

3.3. To the extent that such use of data constitutes processing of personal data, the Data Controller warrants:

a) That the Data Controller has the relevant legal basis for having and processing the personal data, including, if applicable, the relevant permissions from the data subject; and
b) That, if the transfer involves sensitive categories of data, cf. section 3.3, the data subject has been informed or will be informed before the transfer, or as soon as possible after, that its data could be transmitted to a third country not providing adequate protection within the meaning of the Data Protection Legislation.

4. Obligations of the data processor

The Data Processor warrants that the Data Processor will:

a) Comply with the Data Protection Legislation from time to time applicable to the Data Processor's obligations under the Agreement ("Data Protection Legislation"),
b) process any personal data transferred to or collected by the Data Processor only as a 'processor', as such terms are defined in the Data Protection Legislation, on behalf of the Data Controller,
c) Implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the applicable Data Protection Legislation and ensure the protection of the rights of the data subjects,
d) Ensure that Sub-processors follow guidelines to process personal data in accordance with the Data Protection Legislation,
e) Taking into account the nature of the processing, assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the data subject's rights according to the Data Protection Legislation,
f) To a relevant extent assist the Data Controller in ensuring compliance with the requirements for security of personal data,
g) Make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections to facilities under the control of the Data Processor, conducted by the Controller or an auditor mandated by the Controller.

5. Technical and organizational security measures

5.1. The Data Processor will implement and maintain throughout the term of the DPA and will procure its Sub-processors to implement and maintain through the term of the DPA, the appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction, loss, damage or alteration and

against unauthorized disclosure, abuse or other processing in violation of the requirements of Data Protection Legislation.

5.2. The Data Processor will ensure that it and its Sub-processors involved in the processing of personal data always comply with the minimum data security requirements set out in **Appendix 2.**

6. Personnel

6.1. The Data Processor will procure that any personnel of the Data Processor required to access personal data have committed themselves to the obligation of confidentiality set out in the Agreement or are under a statutory obligation of confidentiality.

6.2. The Data Processor will procure that all personnel of the Data Processor required to access personal data are informed of the confidential nature of the personal data and the security procedures applicable to the processing of or access to the personal data.

6.3. The Data Processor's personnel's undertaking to abide by such confidentiality requirements will continue after the end term of this DPA.

7. Assistance to the data controller

7.1 The Data Processor shall provide reasonable and timely assistance to Data Controller to enable Data Controller to respond to:

a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and
b) any other correspondence, inquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. If any such request, correspondence, inquiry, or complaint is made directly to Data Processor, Data Processor shall promptly inform Data Controller providing full details of the same.

7.2 The Data Processor shall provide Data Controller with reasonable cooperation to enable Data Controller to conduct any data protection impact assessment that it is required to undertake under Applicable Data Protection Law.

8. Sub-processors

8.1. The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR to engage another processor (a Sub-processor).

8.2. With this DPA, the Data Processor has the Data Controller's general authorization for the engagement of Sub-processors for the purpose of performing the obligations set out under the Agreement. The Sub-processors, approved by the Data Controller by taking the CC4ALL Services into use, are listed in **Appendix 3**. The Data Processor shall;

a) Maintain an up-to-date list of its Sub-processors within this data processing agreement, published on Data Processors website at https://contactcenter4all.com/ (or any future website used by the Data Processor);
b) Update this Data Processing Agreement Sub Processors list, described in **Appendix 3** with details of any change in Sub-processors at least 30 days prior to any such change (except to the extent a 30 days' notice is not possible due to an emergency). Additionally, the Data Processor will notify the Data Controller of such changes via E-mail.
c) Provide a copy upon request of the data processing agreement(s) between the Data Processor and the Sub-processors at any given time to the Data Controller.

8.3. The Data Controller may object to such new Sub-processor if such addition would cause the Data Controller to violate applicable legal requirements. In the case of a justified objection, the Parties shall negotiate in good faith to find an alternative solution. If such alternative solution cannot be found and the Data Processor decides to proceed with such Sub-processor, the Data Controller can terminate the Agreement with a notice of 30 days. Neither of the Parties shall be considered in breach of contract in the event of such termination.

9. Transfer of data to third countries or international organizations

9.1. Any transfer of personal data to third countries or international organizations by the Data Processor shall only occur based on documented instructions from the Data Controller and shall always take place in compliance with Chapter 5 GDPR.

9.2. If any Data Controller Data originates from any country (other than an EEA country) with one or more laws imposing data transfer restrictions or prohibitions and Data Controller has informed Data Processor of such data transfer restrictions or prohibitions, Data Controller and Data Processor shall ensure appropriate transfer mechanism (satisfying the country's data transfer requirement(s)) is in place, as reasonably requested by Data Controller and mutually agreed upon by both Parties, before transferring or accessing Data Controller's Data outside of such country. For the

avoidance of doubt, this transfer restriction does not pertain to Data Controller or its Affiliates' Authorized Users who have access to the CC4ALL Services and Data Controller Data, and Data Processor shall not be held responsible for actions of Data Controller or its Affiliates' Authorized Users. Neither Data Controller nor its Authorized Users shall be entitled to use the CC4ALL Services or Subscription Services in any country with data localization laws that would require Data Controller's environment to be hosted in said country.

10. Obligations of the data controller

10.1. The Data Controller and the Data Processor will be separately responsible for conforming with the Data Protection Legislation as applicable to them.

10.2. The Data Controller shall be responsible, among others, for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

10.3. The Data Controller will inform the Data Processor in writing without undue delay following the Data Controller's discovery of a failure to comply with Data Protection Legislation with respect to processing of personal data in accordance with this DPA.

10.4. The Data Controller shall be responsible for providing accurate and relevant contact details after entering into the Agreement and thereafter to assist in Data Processor's notification obligations.

10.5. Rights regarding automated decision-making, including profiling: CC4ALL does not utilize customer data to operate its CC application and does not engage in specific profiling activities to support and expand our business.

11. Notification of data breach

11.1. The Data Processor shall notify the Data Controller without undue delay in writing upon identifying any actual or suspected personal data breach related to the processing under this DPA. The Data Processor will act promptly to support the Data Controller in meeting its legal obligations under applicable data protection laws.

11.2. The notification referred to in section 10.1. must, to the extent possible:

a) Describe the nature of the personal data breach including where possible (e.g., loss, theft, copying), the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

b) Communicate the name and contact details of the person with the Data Processor where more information can be obtained,
c) Describe the likely consequences of the personal data breach, and
d) Describe the measures taken or proposed to be taken by the Data Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

12. Additional assignments

12.1. The Data Processor shall carry all costs associated with compliance of this DPA in its capacity as Data Processor.

12.2. The Data Controller shall carry all costs associated with compliance of this DPA in its capacity as Data Controller.

12.3. In respect of tasks of the Data Processor, that are not an obligation under this DPA, cf. the sections above, the Data Processor shall be entitled to charge the Data Controller for the additional resources, time and material necessary to fulfill the required task(s), unless such services are already included in the services rendered under the Agreement.

12.4. The Data Processor will notify the Data Controller in advance of such additional charges and, to the extent possible, provide the Data Controller with a quote of the expected costs.

12.5. If the Data Controller cannot agree to the costs, the Data Processor shall be entitled not to perform the additional assignment and to terminate the Agreement with a notice of 30 days. The Data Processor shall not be considered in breach of contract in this event.

13. Deletion and return of personnel data

13.1. Following the end term or termination of the Agreement, the Data Processor shall (at Data Controller's election) destroy or return to Data Controller all Data in its possession or control. The Data Processor reserves the right after 90 days to delete personal data from all locations when the Data Controller has not elected either option. This requirement shall not apply to the extent that Data Processor is required by applicable law to retain some or all their Data.

13.2. Upon the Data Controller's request, the Data Processor shall certify in writing the destruction of the personal data.

13.3. Upon the Data Controller's request, the Data Processor will delete or anonymize any personnel data stored for specific telephone numbers provided by the Data Controller.

13.4. When Data Controller's request is received, the Data Processor will execute this request within one month from the recorded date of the request.

13.5. The Data Processor will maintain a record of requests for data and the receipt thereof including dates, record and location.

14. Liability

14.1. Each party's liability for one or more breaches of this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement. In no event shall either party's liability for a breach of this DPA exceed the liability cap set out in the Agreement. Neither party limits nor excludes any liability that cannot be limited or excluded under applicable law (such as for fraud).

15. Legal venue and applicable law

15.1. This DPA shall be governed by Dutch Law.

15.2. Any claim or dispute arising from or in connection with the Data Processing Agreement must be settled by The Netherlands Commercial Court (NCC) as first instance.

16. Signatures

Signed for and on behalf of the Data Processor
Date: April 29, 2021

Name: Cees de Jong
Title: CEO

Appendix 1: Information about the processing

1. **The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:**
   The Data Processor is a software development company, assigned by the Data Controller to provide software as a service which contains customer contact functionalities. The content of this DPA reflects personal data the Data Processor handles for the Data Controller.

2. **The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):**
   Offer customer contact channels to customer relations of the Data Controller and route the communication to the Data Controller's employees to handle customer contact.

3. **The processing includes the following types of personal data about data subjects:**
   Name, E-mail address, username, password, telephone number, SIP address, IP address, Microsoft Teams/Skype for Business presence, call data & statistics, call recordings, voicemails

   Personal data processed by the Data Processor is provided primarily by the Data Controller and may additionally originate from end users when they interact with the Data Controller through the communication channels supported by the CC4ALL Services. Certain technical data may also be generated automatically through the use of the CC4ALL Services.

4. **The processing includes the following type of special categories of data about data subjects:**
   Data collected by ContactCenter4ALL does not contain special categories of data in general. Exceptions could occur when certain recording functionalities are enabled and conversations containing special categories of information are being recorded.

5. **Processing includes the following categories of data subject:**
   Data Controller's employees
   Data Controller's customer relations

6. **The Data Processor's processing of personal data is in the following location(s), including name of country/countries of processing:**
   Vianen, The Netherlands
   Iași, Romania

   CC4ALL deploys customer environments in Microsoft Azure regions that match the customer's geographic location. This ensures compliance with data residency regulations and guarantees high availability through region redundancy.

   Europe:
   Azure West Europe, The Netherlands
   Azure North Europe, Ireland

   AMER:
   Azure US, North America
   Azure US3, North America

   APAC:
   Azure South East Australia, Australia
   Azure South Australia, Australia

7. **The Data Processor's processing of personal data on behalf of the Data Controller may be performed when the Clauses commence. Processing has the following duration:**
   The retention policy of personal data is determined specifically per data object. For most data objects a retention of 60 days has been set as a maximum. In some cases, personal data will not be removed but pseudonymized to be able to continue to provide the Data Controller with statistics. On request of the Data Controller, the Data Processor can provide a detailed list with all data object categories and their retention period.

   If for any reason personal data is stored longer than the determined retention policy, the Data Processor will store that personal data until the Data Controller requests that the data is erased or returned, cf. clause 13.1 of this DPA.

Appendix 2: Description of minimum data security

1. **Technical and organizational measures baseline Physical Access Controls**
   Data Processor shall take reasonable measures to prevent physical access, such as secured buildings, to prevent unauthorized persons from gaining access to personal data.

2. **System Access Controls**
   Data Processor shall take reasonable measures to prevent personal data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords, role-based access control and logging of access on several levels.

3. **Data Access Controls**
   Data Processor shall take reasonable measures to provide that personal data is accessible and manageable only by properly authorized staff. Application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the personal data to which they have privilege of access; and, that personal data cannot be read, copied, modified or removed without authorization in the course of processing. The Data Processor shall take reasonable measures to implement an access policy under which access to its system environment, to personal data and other data by authorized personnel only.

4. **Transmission Controls**
   Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. **Input Controls**
   Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified, or removed. Data Processor shall take reasonable measures to ensure that (i) the personal data source is under the control of data exporter; and (ii) personal data integrated into Data Processor's systems is managed by secured file transfer from the Data Processor and data subject.

Appendix 3: Authorized Sub-Processors

1. **Sub-Processors on behalf of the Data Processor are:**
   Expert Network
   Barbu Lăutaru 11, 700399 Iași, Romania
   Software Development, Tier 3 Support

   Hostersi Sp. z o.o.
   Jankowicka 7, 44-200 Rybnik, Poland
   Cloud Infrastructure

2. **The purpose of the Sub-Processors processing of personal data on behalf of the Data Processor is:**
   The by the Data Processor assigned Sub-Processors providing several services to the Data Processor. These services are deployed to maintain and improve confidentiality, integrity, availability, support, and development of the Data Processor services.

3. **The Data processor and Sub-Processors have mutual agreements for the processing of the personal data from the Data Controller**
   A Business Partner Agreement (BPA) describing that their mutual goal is to provide Customer Contact services to the Data Controller and their customers.
   Security processing documentation describing how to maintain confidentiality, integrity, availability, and how to jointly process the data of the Data Controller following security standards when using, implementing, and developing Data Processors services.

4. **The Data processor and Sub-Processors have agreed that:**
   Sub-Processors will only access data on behalf of ContactCenter4ALL or with permission from ContactCenter4ALL. Sub-Processors will always handle data diligent and make sure the processes to develop, manage and maintain the CC4ALL Services and architecture used by the Data Controller are GDPR compliant.