Appendix 2

DATA PROCESSING AGREEMENT-DPA

DATE: 27-06-2018

BETWEEN

Supplier

Moranti Services A/S
Bådehavnsgade 2A
DK-2450 København SV
Company No. 38145622

Referred to as the data processor

Customer

Navn
Adresse
Postnr og by
Company No.

Referred to as the data controller

1. Background

Inbound
The data controller wants the data processor to handle incoming calls per phone/mail/social media on behalf of the data responsible. The calls are answered/transferred/forwarded/recorded according to the contractually agreed terms.

Outbound
The data controller wants the data processer, by phone, to handle the verification of leads delivered by the data controller. This includes information of people who have consented to be contacted by phone, of the data responsible. All calls are recorded as contractually agreed.

For this purpose, the data processor will during the term of the Framework Agreement be processing personal data on behalf of the data controller.

The data processor will be processing the following type of personal data under the Framework Agreement:

i. [Please list the applicable types of personal data, e.g. name, address, health data, criminal records etc.]

The personal data regards the following categories of data subjects:

ii. [Please list the categories of data subjects, e.g. employees, customers, health professionals etc.]

2. Definitions

The data processor is acting according to the instructions of the data controller. The data controller determines the purposes and how the processing of personal data should be handled.

Any terms not otherwise defined in the Framework Agreement shall be interpreted to have the meaning ascribed to them in the provisions laid down in the Applicable Data Protection Laws (as defined below). "Applicable Data Protection Laws" mean any applicable law relating to data protection and security, including without limitation EU Data Protection Directive (EU Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) , Directive on privacy in electronic communications (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) and General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 94/46/RC, the "GDPR") and any amendments, replacements or renewals thereof, all binding national laws implementing the EU Legislation and other binding data protection or data security directives, laws, regulations and rulings valid at the given time.

"International Data Transfer" means transfer of personal data to recipients outside the EU Member State or EEA Countries ("third country") being understood that personal data transfer shall include transfer of personal data as such as well as access made available to personal data.

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be directly or indirectly identified by reference to an identifier such as a name, address, social security number, subscription number, IP address, location data, an online identifier, traffic data or message content or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Security Requirements" means all agreed applicable security requirements and security instructions and their updates applicable at each point in time depending on the nature of the Deliverables to be provided by Data Processor. Security Requirements include:

(i) the Security provisions of the Agreement
(ii) the Security Directives
(iii) Further security instructions as provided by Data Controller from time to time

3. Restrictions

The data processor shall only process personal data in accordance with the instructions of the data controller, unless the data processor is required to process the personal data to comply with European Union or Member State law to which the data processor is subject. In that case, the data processor shall inform the data controller hereof before the data controller processes the data.

The data controller determines the purposes and how the processing of personal data should be handled, and the data processor shall process personal data for the limited purpose of performing the obligations set out under the Framework Agreement.

The data processor will immediately inform the data controller if, in its opinion, an instruction infringes the Applicable Data Protection Laws.

4. Security

The data processor will implement appropriate technical and organizational security measures in order to protect data against accidental or unlawful destruction, loss or alteration and against the unauthorized disclosure, abuse or other processing in violation of the law concerning the processing of personal data.

The data processor shall also ensure that it and its subcontractors/sub-processors involved in the processing of personal data at all times comply with such security requirements.

Upon request from the data controller, the data processor must immediately provide adequate information to enable the data controller to assess and verify that the necessary security measures are implemented

and complied with, as needed for the data controller to demonstrate compliance with the security provisions in the Applicable Data Protection Laws.

By own initiative, the data processor is obliged to seek clarification of any doubt on security requirements and fulfilment, including contact to the data responsible.

Upon the data controller's written request, the data processor shall permit the data controller or any third party appointed by the data controller (subject to reasonable and appropriate confidentiality undertakings), to audit the data processor's data processing activities and compliance with all reasonable requests or directions by the data controller to enable the data controller to verify and/or procure that the data processor and/or subcontractors/sub-processors are in full compliance with their obligations under the Framework Agreement and the Applicable Data Protection Laws. Unless required by the Applicable Data Protection Laws or a data breach has occurred, no audits will be conducted more than once in any twelve (12) month period.

The data processor shall in accordance with the data controller's instructions on an annual basis provide to the data controller an audit report covering control of the technical and organisational security measures implemented by the data processor and any sub-processors (such as ISAE 3000) which will be prepared by a reputable independent third party that attests to the compliance of the applicable security controls, and upon the data controller's request complete a security questionnaire submitted by the data controller to the data processor.

The data processor must upon the request of any public authority, grant the authority access to perform an auditing or other investigations of the processing of personal data conducted by the data processor. The data processor shall without undue delay inform the data controller in writing upon receiving such request, unless this is expressly prohibited by the public authority.

The data processor shall without undue delay notify the data controller of a data subject's request to exercise his/her rights under the Applicable Data Protection Laws, forward the request to the data controller and provide full cooperation and assistance in relation to the data controller's obligation to respond to said request.

Special attention to:

Collecting the data must not be stored longer than necessary for the purposes for which they were collected.

Persons, of whom data are collected, are entitled to be informed for what purpose the data are collected.

The information may not be disclosed to third parties, unless required by existing legislation or on instructions from the data controller.
The data processor will ensure that only persons, who are authorized by the data processor, have access to the personal data processed.
Furthermore, the data processor must ensure that such persons processing personal data on its behalf have committed themselves to obligations of confidentiality regarding any personal data processed. The obligation of confidentiality will continue after the termination of the Framework Agreement.

When processing data outside of the data processor' premises, including the use of home offices or the like, ensures the data processor that the necessary technical and organizational security are complied.

The data processor must not transfer personal data out of the European Economic Area (the "EEA") without the prior written approval of the data controller. In the event such approval is granted, the data processor must comply with any requirements established by any data protection authority or any other governmental authorities necessary for the granting of approval by such authorities for the transfer of personal data outside of the EEA, including by facilitating the conclusion of the Commission's standard contractual clauses.

Deleting data media due to repair, replacement, scrapping and sale of data media must be performed efficiently by overwriting with a special program, destruction or demagnetization of the data medium.

5. Data Breach Notification

The data processor shall without undue delay and no later than within a timeline allowing the data controller to comply with the Applicable Data Protection Laws in writing notify the data controller in case of any identified or potential breach of personal data processed under the Framework Agreement. The notification shall include any other information required in order for the data controller to comply with the Applicable Data Protection Laws, including information about the nature of the breach and measurements taken to control it. The data processor shall assist the data controller with communication of any personal data breach to the affected data subjects and relevant authorities.

6. Changes

At any time and without further notice, this data processing agreement can be changed if the changes are necessary to comply with the applicable rules and regulations for the processing of personal data.

7. Subcontractors

The data processor shall not sub-contract any of its processing operations performed on behalf of the data controller to another data processor (sub-processor) without the prior written consent of the data controller. The data processor is obliged to provide any and all documentation and information required for the data controller to assess the suggested sub-processor and determine if the suggested sub-processor is suitable.

The data processor uses the following subcontractors/sub-processors, when entering into this Framework Agreement, for the purpose of solving the contractual obligations on behalf of data controller and approved by the data processor. The following subcontractor/sub-processor shall be deemed accepted by the data controller:

Lytzen IT A/S
Aalborgvej 94
9800 Hjørring, Denmark
Company-No: 26195403

Technical Support including fault correction in accordance with Service Level Agreements (SLA)/ Maintenance & Support Agreements (M&S). Hosting and contact center management.

8. Signatures

This Appendix 2 is signed in two (2) identical copies of which each party retain a copy.

Date: / 20	Date: / 20
Moranti Services A/S	**Customer**
_____	_____
Birgitte Dam Kræmmergaard	xxxxxxxxx
CEO	xxxxxx
_____	_____