PERSONAL DATA PROCESSOR AGREEMENT

Between **and Telavox**

Between **Telavox Group**, including its affiliates **Telavox AB** (Corp. Reg. No. 556600-7786), **Telavox ApS**(Corp. Reg. No. 36079762), **Telavox AS** (Corp.Reg.No 915639275) and **Telavox Oy** (2814794-4) hereinafter referred to as the **Personal Data Processor** and Corp. Reg. No. hereinafter referred to as the **Personal Data Controller**, the following Personal Data Processor Agreement ("**Processor Agreement**") has been entered.

The Personal Data Controller and the Personal Data Processor are hereinafter referred to as the **Party** or jointly the **Parties**.

1. DEFINITIONS

1.1 The terms used in this Processor Agreement shall be deemed to have the same meaning as in the applicable data-protection regulations and the practice developed at any given time regarding the applicable data-protection regulations. This means that definitions in this Processor Agreement may change during the term of the agreement. The above means that this Processor Agreement involves the following definitions:

Processing: The measure or combination of measures concerning Personal Data or sets of Personal Data, e.g. collection, registration, organisation, structuring, storage, processing or alteration, creation, reading, use, surrender through transfer, dissemination or other provision, adjustment or consolidation, limitation, deletion or destruction.

Applicable data-protection regulations: Council Directive 95/46/EC, introduced into Swedish law through the Swedish Personal Data Act (1998:204) and the Swedish Personal Data Ordinance (1998:1191) and the General Data Protection Regulation (EU) 2016/679 ('GDPR'), with the relevant implementation statutes and the regulations in this area applying at any given time. In the event of a conflict between the above-mentioned statutes, GDPR shall take precedence as from 25th May 2018.

Personal data: any information relating to any living identified or identifiable natural person.

Personal-data breach: security incidents leading to unintentional or unlawful destruction, loss or alteration, or to unauthorised disclosure of or unauthorised access to the Personal Data that has been transferred, stored and otherwise been the subject of Processing.

Sub-processor: any personal-data processor engaged by the Personal Data Processor that processes Personal Data on behalf of the Personal Data Controller.

2. BACKGROUND AND PURPOSE

2.1 The Personal Data Processor develops, produces and sells fixed and mobile IT and communications solutions, hardware and software, and thereby carries out compatible operations of which processing of Personal Data constitutes a natural part.

2.2 The Personal Data Processor will process Personal Data for the Personal Data Controller. The processing the Personal Data Processor will perform on behalf of the Personal Data Controller shall be regulated by this Processor Agreement.

2.3 On the basis of the above, the Parties have entered into the following Processor Agreement.

3. RESPONSIBILITY OF THE PERSONAL DATA CONTROLLER

3.1 The Personal Data Controller shall ensure that the processing of Personal Data complies with applicable data-protection regulations.

3.2 The Personal Data Controller may only provide the Personal Data Processor with the Personal Data necessary for the purpose of the processing.

3.3 The Data Processing Controller shall immediately provide the Personal Data Processor with correct information in the event of the instructions being incorrect, incomplete or otherwise in need of alteration.

4. PROCESSING OF PERSONAL DATA

4.1 The Personal Data to which the Personal Data Processor has access may only be processed in accordance with this Processor Agreement and the applicable data-protection regulations, as well as the Personal Data Controller's documented instructions applying at any given time (see Annexe 1).

4.2 The Personal Data Processor shall immediately notify the Personal Data Controller if the Personal Data Processor considers that an instruction issued by the Personal Data Controller is in breach of applicable data-protection regulations.

4.3 The Personal Data Processor shall without undue delay but no later than thirty (30) days as from the request on the part of the Personal Data Controller give the latter access to Personal Data in the possession of the Personal Data Processor, and shall carry out the requested amendment, deletion, limitation or transfer of such Personal Data, unless this is incompatible with mandatory legislation. If the Personal Data Controller has deleted data or instructed the Personal Data Processor with regard to deletion, the latter shall undertake the requisite measures to ensure the deleted Personal Data cannot be restored.

4.4 The Personal Data Processor shall always and without any special request from the Personal Data Controller undertake the measures referred to in 4.3 if this follows from the instructions in Annexe 1.

4.5 The Personal Data Processor shall maintain a written register of all Processing of Personal Data carried out on behalf of the Personal Data Controller, and at the express request of the Personal Data Controller or the relevant supervisory authority shall submit a legible register extract that as a minimum includes details of:

a) the name and contact details of the Personal Data Processor and, where applicable, the Personal Data Processor's representative, the data-protection officer and, where appropriate, the hiring of a Sub-processor;
b) the processing carried out by the Personal Data Processor on behalf of the Personal Data Controller and on behalf of any other personal data controller, the type of Personal Data and, where appropriate, the specific categories of Personal Data processed;
c) where appropriate, transfer of Personal Data to a third country, the third country where data is processed and the appropriate safeguards undertaken, and
d) a general description of the technical and organisational measures undertaken to maintain an appropriate level of protection;

5. CAPACITY AND CAPABILITY

5.1 The Personal Data Processor guarantees possession of the requisite technical and organisational capacity and capability, including technical solutions, expertise, financial and human resources, procedures and methods for meeting its obligations

under this Processor Agreement and the applicable data-protection regulations.

5.2 At the request of the Personal Data Controller or a third party hired by the Personal Data Controller, the Personal Data Processor shall certify that the obligations arising from this Processor Agreement and the applicable data-protection regulations are met by providing the relevant documentation, referring to a relevant and approved code of conduct or certification, enabling and contributing to audits and inspections of premises, IT systems and other assets and/or providing appropriate evidence without undue delay.

6. SECURITY AND CONFIDENTIALITY

6.1 The Personal Data Processor shall undertake the requisite measures for compliance with the security requirements in conjunction with the processing of Personal Data in accordance with applicable data-protection regulations, which can include but are not limited to pseudonymisation and encryption of Personal Data, the capacity to continuously ensure the integrity and resilience of the systems and services and the capacity to restore availability of and access to Personal Data within a reasonable period of time in the event of a physical or technical incident.

6.2 By means of appropriate technical and organisational measures the Personal Data Processor shall restrict access to the Personal Data and only grant access to staff who need access to the Personal Data in order to meet their obligations under this Processor Agreement, ensure that such staff have the requisite training and have been provided with sufficient instruction for handling of the Personal Data in an appropriate and secure manner, and ensure that the staff only process the Personal Data when the Personal Data Controller has been instructed so to do, and then in accordance with the instructions provided by the Personal Data Controller.

6.3 The Personal Data Processor shall process Personal Data confidentially and shall ensure that persons authorised to process the Personal Data at the Personal Data Processor's have entered into a special confidentiality agreement or been informed that a special professional secrecy obligation applies in accordance with an agreement or applicable legislation.

6.4 The Personal Data Processor shall, without undue delay but at the latest within seventy-two (72) hours as from its coming to the notice of the Personal Data Processor, notify the Personal Data Controller of the existence or risk of a personal-data breach. Such a notification shall include all the available information the Personal Data Controller requires in order to undertake appropriate preventive measures and countermeasures and to meet its obligations regarding reporting of Personal-Data breaches to the relevant supervisory authority.

7. COLLABORATION

7.1 If the Personal Data Controller makes an enquiry in this regard, the Personal Data Processor shall assist the latter in meeting its obligations under the applicable data-protection regulations, e.g. performance of data-protection impact assessments, design of appropriate technical and organisational measures regarding built-in data protection, prior consultation with the relevant supervisory authority, and shall assist in investigating any personal-data breaches that have occurred. In view of the nature of the processing, the Personal Data Processor shall as far as possible also assist the Personal Data Controller by means of appropriate technical and organisational measures, so the Personal Data Controller can meet its obligation to comply with the registered party's request for transparency, information on and access to Personal Data, deletion, rectification, restriction of processing or portability or any other request in accordance with the applicable data-protection regulations on exercising of the registered party's rights. Unless agreed otherwise by the Parties, the assistance referred to in this paragraph shall not give the Personal Data Processor

the right to special remuneration.

7.2 The Personal Data Processor shall without undue delay notify the Personal Data Controller if the latter is contacted by the relevant supervisory authority or other third party for the purpose of gaining access to Personal Data in the possession of the Personal Data Processor or, where applicable, the Sub-Processor.

7.3 The Personal Data Processor shall issue the Personal Data Controller with advance notice in writing of any planned changes to the processing of Personal Data, including technical and organisational changes that may affect the protection of the Personal Data and the Personal Data Processor's compliance with applicable data-protection regulations. Prior to implementation of such changes the Personal Data Controller shall issue written consent, which shall not reasonably be denied.

8. HIRING A SUB-PROCESSOR

8.1 The Personal Data Processor shall not hire another personal-data processor without having obtained special or general prior written authorisation from the Personal Data Controller. Such a transfer will not entail any changes to the division of responsibilities between the Parties to this Processor Agreement.

8.2 If the Personal Data Processor transfers the processing of Personal Data to the Sub-Processor, then the Personal Data Processor shall ensure by written agreement that there are guarantees from the Sub-Processor that this complies with all the applicable provisions regarding protection for Personal Data, and that it meets all the obligations regulated in this Processor Agreement. The Personal Data Processor shall be fully accountable to the Personal Data Controller in terms of the Sub-processor meeting its obligations regarding the applicable data-protection regulations.

8.3 If the Personal Data Processor intends to replace an existing Sub-processor with another Sub-processor, then the Personal Data Processor shall at the latest thirty (30) days beforehand notify the Personal Data Controller of its intentions, so the Personal Data Controller is able to object to such a change. If the Personal Data Controller on reasonable grounds opposes replacement of the Sub-processor or revokes its prior consent regarding use of the Sub-processor, then the Personal Data Controller has the right to terminate this Processor Agreement and other agreements entered into concerning processing of Personal Data. During the period of notice there must be no transfer of Personal Data to another Sub-processor.

9. TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

9.1 If in conjunction with the Processing the Personal Data Processor intends to transfer Personal Data to a third country outside the EU/EEA that is not deemed by the European Commission to exercise an appropriate level of protection in relation to the applicable data-protection regulations, then prior to transfer the Parties shall enter into a written supplementary agreement concerning such a transfer.

9.2 If the Personal Data Processor has hired a Sub-processor, and the latter intends to transfer Personal Data to a third country that the European Commission does not deem to have an appropriate level of protection in relation to applicable data-protection regulations, then prior to transfer the Personal Data Processor and the Personal Data Controller must enter into a written supplementary agreement in this regard. Before a transfer can take place, the Personal Data Processor and the Sub-processor must also entered into a written supplementary agreement involving the same terms & conditions. The Personal Data Processor shall provide the Personal Data Controller with a signed copy of the supplementary agreement between the Personal Data Processor and the Sub-processor before such a transfer may take place.

10. **NOTIFICATIONS**

10.1 If a personal-data breach occurs or is feared, then the Personal Data Processor must report to

11. **VALIDITY**

11.1 This Processor Agreement is valid until the Personal Data Processor's processing of the Personal Data ceases, this Processor Agreement is replaced by another Personal Data Processor Agreement or the Personal Data Controller terminates the Processor Agreement in accordance with 8.3. In the event of termination in accordance with 8.3, a period of notice of two months shall apply to the Processor Agreement as well as to other agreements terminated in conjunction with termination of the Agreement.

11.2 Upon completion of processing, the Personal Data Processor shall return the Personal Data to the Personal Data Controller in a general and legible format, and shall thereafter delete the Personal Data from systems used for processing, unless this is incompatible with other mandatory legislation.

12. **APPLICABLE LAW AND DISPUTES**

12.1 This Processor Agreement shall be interpreted and applied in accordance with the same law as stated in the Terms and Condition for the purchased Service.

This Processor Agreement is valid as from 25th May 2018. This Processor Agreement has been drawn up in two (2) copies, and each party has taken each a copy.

Place	Place
MALMÖ	
Date	Date
26/01/2021	
Personal Data Processor, Telavox	**Personal Data Controller,**
PP - Lasse Nielsen	

ANNEXE 1 INSTRUCTIONS

These instructions form an integral part of the Processor Agreement and shall be adhered to by the Personal Data Processor in the processing of Personal Data, unless expressly state otherwise in the Processor Agreement. The Personal Data Controller may unilaterally change these instructions at a later date by notifying the Personal Data Processor of the change in writing. Changes take effect no earlier than 30 calendar days after having been sent by the Personal Data Controller. By signing the Processor Agreement, the Personal Data Controller Processor has confirmed the meaning of these instructions.

Purpose
The purpose of the processing is
1) to deliver telephony and communication services in accordance with the agreement entered into by the Parties below ('Service Agreement') and services delivered ('Service')
2) to support the Service with which the customer is supplied
3) otherwise discharge responsibilities under the Service Agreement.

Type of processing
Registration of user data, storage of Personal Data, storage of use of the Service, statistical analyses, troubleshooting analyses and invoicing data/documentation.

Type of Personal Data
The following types of Personal Data are processed:

- Name:
- Password
- Email
- User ID
- Phone number
- IP address
- User-generated content, e.g. call information and/or data consumption
- User behaviour, crash reports for troubleshooting
- Billing information

In addition to this, the Personal Data Controller's users can upload Personal Data in a Service, e.g. profile picture, position, address and further contact details. Upon uploading, the Personal Data Controller approves the Personal Data Processor's processing and storage of this information.

Place of processing
All processing takes place within the EU's member states, the EEA or EU-approved states that attain the appropriate level of protection.

Duration of Processing
Processing lasts for as long as the Personal Data Processor represents the Personal Data Controller. Upon termination of the Service Agreement, Personal Data is deleted from active systems and is phased out from backups over time. These backups have limited access, and Personal Data can remain for a maximum of two (2) years.

Sub-processors
The following types of Sub-processors are used

1) Troubleshooting and optimisation of service
   In the event of a fault in the service, some Personal Data is sent to network providers, e.g. Telia Management Systems, for implementation of troubleshooting and Service restoration. Monitoring and statistical monitoring of the Service is performed continuously to facilitate optimisation of use of the Service and identification of any bugs where specific Personal Data is disclosed to Sub-processors such as Google Analytics and Netrounds.
2) DEALERS
   If the Personal Data Controller enters into a Service Agreement through one of the

Personal Data Processor's dealers, then said dealer has access to Personal Data in order to support the Service.

3) Server rooms
   The Sub-processors are used for hosting of servers, and these Sub-processors operate within the EU
4) Response Services
   In certain specific response services, sub-processors are used that then gain access to support tools and certain Personal Data.

Disclosure of Personal Data
Personal Data may be disclosed to:

- Authorities
  On request, and in accordance with the law and official decisions, the Personal Data Processor is obliged to disclose the data resulting from the decision – e.g. to the police.
- Emergency services
  In the event of a call to SOS Alarm, for example.
- Other operators or service providers providing the Service
  When placing calls to another operator, for example, certain Personal Data is registered with said operator.

Personal Data may also be disclosed to other companies and authorities after the Personal Data Controller has given consent, and/or in order to discharge a specific part of the Service under an agreement, e.g. as regards Directory Enquiries operations.

Transfer to third country
Transfer to a third country outside the EU/EEA is only to take place in accordance with Articles 45, 46 or 49 of the General Data Protection Regulation, and the latter only provided that the transfer is necessary for discharge of an agreement between the Personal Data Processor and the Personal Data Controller, or for implementation of measures prior to such an agreement at the registered party's request.

DATA PROTECTION, SECURITY AND CONFIDENTIALITY
The Data Protection Processor has undertaken the requisite technical and organisational measures in order to guarantee the integrity and confidentiality of Data Protection Controller data, which may include the following measures:

Staff Confidentiality
The Data Protection Processor has undertaken the requisite measures in order to guarantee that staff using the Data Protection Controller's Data Protection have the appropriate background and expertise. These measures may include:

- Background checks in the form of references and/or excerpts from criminal records
- Written agreement on professional confidentiality
- Continuous training and skill-enhancing measures

Physical security
The Personal Data Processor ensures maintenance of an appropriate level of physical security in areas where the Personal Data Controller's Personal Data is processed, which may include:

- Limited and/or supervised access to physical premises
- Monitoring in the form of alarms, video and/or physical monitoring

Equipment, system and network security
The Personal Data Processor shall implement appropriate and up-to-date security measures and, for the duration of the Service Agreement, maintain an appropriate level of security for all systems, networks and units used to deliver the Service to the Personal Data Controller. This may include:

- Having appropriate firewall protection
- Audit logging for service monitoring

- Authentication systems for access to Service and systems
- Rights systems for access to Service and systems
- Monitoring & encryption of physical hard drives
- Processes & procedures for continuous evaluation of data security
- Ensuring there are options for restoring Personal Data through backups