Telavox - Data Processing Agreement

Customer and/or Telavox are referred to alone as "**Party**" or jointly as the "**Parties**".

1 DEFINITIONS

The following terms and expressions shall have the meaning set out below. All capitalized terms not de- fined in this DPA will have the meaning given to them in the Agreement.

Terms not capitalized but defined in the GDPR, such as the terms "controller", processor, personal data, "processing" and "personal data breach" shall have the same meaning as defined in the GDPR.

"Agreement" means the telecommunication services agreement, including the Telavox's general terms and conditions and other appendices and any amendments, entered into by the Parties.

"Data Protection Laws" means the General Data Protection Regulation (EU) 2016/679 as amended, consolidated or replaced from time to time (the "GDPR") and any national derogations or supplemental legislation and/or regulations to the GDPR.

"Services" means the telecommunication services to be provided by Telavox as specified in the Agreement.

"Standard Contractual Clauses" shall mean the latest version of the standard contractual clauses adopted by the Commission on the basis of Article 46(2) of the GDPR.

2 INTRODUCTION

2.1 The Parties have entered into the Agreement, under which Telavox will provide telecommunication services. Under the Agreement, Telavox will process personal data on behalf of the Customer.

2.2 This DPA is a supplement to the Agreement. The purpose of this DPA is to ensure compliance with Article 28(3) and (4) of the GDPR. Under this DPA, Telavox will be acting as processor and the Customer as controller.

3 THE PROCESSING

3.1 The details of the processing operations, and in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Customer, are specified in Annex 1.

3.2 Telavox shall process personal data only on documented instructions from the Customer, unless required to do so by Union or Member State law to which Telavox is subject. Such instructions are specified in Annex 1. Subsequent instructions may also be given by the Customer throughout the duration of the processing of personal data, and such instructions are subject to available services under the Agreement as well as applicable fees. Such instructions shall always be documented.

4 OBLIGATIONS OF THE PARTIES

4.1 Each Party undertakes to fulfil their duties as processor and controller, respectively, under the applicable Data Protection Laws.

4.2 Telavox shall deal promptly and properly with all reasonable inquiries from the Customer that relate to the processing under this DPA.

4.3 Telavox shall immediately inform the Customer if instructions given by the Customer, in the opinion of Telavox, infringe the Data Protection Laws.

4.4 The Customer shall without undue delay inform Telavox upon any changes that might affect Telavox's obligations under this DPA.

4.5 Should anyone else, either alone or jointly with the Customer, become the controller(s), the Customer shall inform Telavox thereof.

4.6 The Customer undertakes to notify Telavox in writing in the event of any measures taken by third parties, including but not limited to Supervisory Authorities, relating to Telavox's processing hereunder.

4.7 Telavox undertakes to not disclose or otherwise make the personal data processed under this DPA available to any third party, without the Customer's prior written approval, subject to any order by an authority to disclose the personal data or as required under the Data Protection Laws. Telavox commits to notify the Customer in writing in case of a requirement to disclose information, unless prohibited by such order or applicable law.

5 SECURITY OF PROCESSING

5.1 Telavox shall implement the technical and organisational measures specified in Annex 2 to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (personal data breach). In assessing the appropriate level of security, Telavox shall in particular take due account of the risks involved in the processing, the nature of the personal data and the nature, scope, context and purposes of processing.

5.2 In connection with the Service, the Customer will have access to the Telavox Admin, a web portal where the Customer can manage features and the administration of users themselves. The Customer is responsible for not submitting any special categories of personal data (i.e. sensitive data such as personal data concerning health or racial or ethnic origin) into the Telavox Platform, without first notifying Telavox in writing.

5.3 The Supplier undertakes to provide written instructions to persons acting under the authority of the Supplier, who have access to Personal Data, obliging such persons only to Process the Personal Data only according to documented instructions from the Customer, unless required to do so by Uni- on or Member State law.

5.4 The Supplier undertakes to ensure that persons authorised to process the personal data have undertaken confidentiality obligations and to provide written instructions to such persons acting under

5.5 the authority of the Supplier obliging them only to process the personal data according to documented instructions from the Customer, unless required to do so by Union or Member State law.

6 COMPLIANCE

6.1 The Parties shall be able to demonstrate compliance with this DPA.

6.2 Telavox shall, taking into account the nature of processing and the information available to Telavox, assist the Customer in any way necessary for the Customer to comply with its obligations under Artic- les 32 to 36 of the GDPR. Any assistance requested by the Customer under this DPA shall be subject to such generally applicable professional services fees applied by Telavox from time to time (or as agreed under the Agreement, if applicable).

6.3 Telavox shall assist the Customer in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to Telavox:

i. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a "data protection impact assessment") where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

ii. the obligation to consult the competent supervisory authority (where relevant the Swedish Authority for Privacy Protection, IMY), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Customer to mitigate the risk.

7 PERSONAL DATA BREACH

7.1 In the event of a personal data breach concerning data processed by Telavox, Telavox shall notify the Customer without undue delay and at the latest within 48 hours after having become aware of the breach. Such notification shall contain the details of a contact point where more information concerning the personal data breach can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and data records concerned), its likely consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall be provided as it becomes available without undue delay.

7.2 Telavox shall cooperate in good faith with and assist the Customer in any way necessary to enable the Customer to notify, where relevant, the competent data protection authority and the affected data subjects, taking into account the nature of processing and the information available to Telavox.

7.3 Telavox shall assist the Customer in notifying the personal data breach to the competent supervisory authority (where relevant the Swedish Authority for Privacy Protection, IMY.) Telavox shall be required to assist in obtaining in particular the following information which, pursuant to Article 33(3) GDPR, shall be stated in the Customer's notification:

i. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
ii. the likely consequences of the personal data breach;
iii. the measures taken or proposed to be taken by the Customer to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8 DATA SUBJECT RIGHTS

8.1 Taking into account the nature of the processing hereunder, Telavox shall assist the Customer in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights, by appropriate technical and organisational measures, insofar as this is possible.

8.2 Telavox shall promptly notify the Customer about any request received directly from the data subject, and shall not respond to that request itself and shall not respond to that request itself.

9 SUB-PROCESSORS

9.1 The Customer hereby approves a general authorisation for Telavox to engage sub-processors. The list of sub-processors the data processor is currently using is available through the following link (https://telavox.com/gdpr/terms/subprocessors), which are hereby approved by the Customer. Telavox shall in- form in writing the Customer of any intended chang- es of that list through the addition or replacement of sub-processors at least 30 (thirty) days in advance, thereby giving the Customer the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s) within 14 days from being notified. If Customer does not provide an objection within this timeframe, Customer is deemed to accept the respective sub-processor.

9.2 If Customer objects to the use of a sub-processor for legitimate and reasonable reasons relating to privacy or data security, Telavox will use reasonable efforts to work in good faith with Customer to find an acceptable, commercially reasonable, alternate solution. If the Parties are not able to agree to an alternate solution within a reasonable time (no more than 30 days from Telavox's receipt of notice of Customer's objection), Telavox will either not appoint or replace the sub-processor or, if this is not possible, Customer may suspend or terminate the applicable order for Services in respect only to the specific Services which cannot be provided by Customer without the use of the objected-to new sub-processor, by providing written notice to Telavox and without prejudice to any fees incurred by Customer prior to suspension or termination.

9.3 In the event that the Customer provides an objection to a new sub-processor and such objection in Telavox's opinion prevents effective provision of Telavox's services, then Telavox may terminate the Agreement without penalty or liability.

9.4 Where Telavox engages a sub-processor for carrying out specific processing activities (on behalf of the Customer), it shall do so by way of a contract which imposes on the sub-processor the same obligations as the ones imposed on the data

processor under this DPA. Telavox shall provide, at the Customer's request, a copy of such a sub-processor agreement and subsequent amendments to the Customer. Telavox shall ensure that the sub-processor complies with the obligations to which the data processor is subject pursuant to this DPA and to the GDPR.

9.5 Telavox shall remain fully responsible to the Customer for the performance of the sub-processor's obligations under its contract with Telavox. Telavox shall notify the Customer of any failure by the sub-processor to fulfil its obligations under that agreement.

10 INTERNATIONAL TRANSFERS

Any transfer of data to a third country or an international organisation by Telavox shall be undertaken only in compliance with Chapter V of the GDPR.10.2 Telavox agrees that where it engages a sub-processor in accordance with Section 9 above for carrying out specific processing activities (on behalf of the Customer) in a third country and those processing activities involve transfer of personal data within the meaning of Chapter V of the GDPR, Telavox and the sub-processor may use Standard Contractual Clauses in order to comply with the requirements of Chapter V of the GDPR, provided the conditions for the use of those clauses are met.

11 AUDITS

11.1 Telavox shall make available to the Customer all information necessary to demonstrate compliance with the obligations set out in this DPA and that are stemming directly from the GDPR and at the Customer's request, allow for and contribute to reviews of data files and documentation or of audits of the processing activities covered by this DPA, in particular if there are indications of non-compliance.

11.2 The Customer may choose to conduct the audit by itself, to mandate, at its own cost, an independent auditor or to rely on an independent audit mandated by the Customer. Where the Customer mandates an audit, the Customer has to bear the costs of the independent auditor. Prior to an audit or inspection a detailed plan on scope, duration and start date of the audit shall be agreed in writing between the Parties. The Customer's notification for an audit shall include such a proposed plan.

11.3 Nothing in this Section 11 shall entitle the Customer, or any auditor, to access activities, records, information or any other material in any form (i) relating to other clients of the Supplier, (ii) not relevant to the processing of the personal data, (iii) which is commercially sensitive information, or (iv) which is legally privileged or subject to confidentiality obligations (either by law or contract) owed by Telavox to a third party.

11.4 Telavox and the Customer shall make the information referred to in this Section 11, including the results of any audits, available to the competent supervisory authority on request.

12 TERM AND TERMINATION

12.1 This DPA enters into force on the effective date of the Agreement and remains in force until termination of the Agreement.

12.2 Without prejudice to any provisions of the GDPR, in the event that Telavox is in breach of its obligations under this DPA, the Customer may instruct Telavox to temporarily suspend the processing of personal data until Telavox complies with this DPA or the Agreement is terminated. Telavox shall promptly inform the Customer in case it is unable to comply with this DPA, for whatever reason.

12.3 The Customer shall be entitled to terminate this DPA where:

i. the processing of personal data by Telavox has been temporarily suspended by the Customer pursuant to Clause 12.2 above and compliance with this DPA is not restored within a reasonable time and in any event within one month;
ii. Telavox is in substantial or persistent breach of this DPA or its obligations under the GDPR;
iii. Telavox fails to comply with a binding decision of a competent court or the competent supervisory authority (where relevant the Swedish Authority for Privacy Protection, IMY) regarding its obligations under this DPA or under the GDPR.

13 EFFECTS OF TERMINATION

13.1 Processing by Telavox shall only take place for the duration of the Agreement. Upon termination of the provision of personal data processing services or termination pursuant to Section 12, Telavox shall delete all personal data processed on behalf of the Customer and delete existing copies unless Union or Member State law requires storage of the personal data.

14 LIABILITY

14.1 The Parties shall be liable towards each other for any direct damages, costs and losses, including ad- ministrative sanctions incurred due to the breaching Party's violation of this DPA and the breaching Party shall compensate the other Party for any such damage, cost or loss.

14.2 Notwithstanding the above, no Party shall be held liable for indirect losses, including damages and/or consequential damages such as loss of profit or revenue, or other economic losses incurred pursuant to this DPA. Any claim or remedies the Customer may have against Telavox arising under or in connection with this DPA will be subject to the limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement.

15 MISCELLANEOUS

15.1 In the event of a conflict between this DPA and the Agreement, this DPA shall prevail.

15.2 Any changes or supplements to this DPA shall, in order to be effective, be made in writing and signed by both Parties.

15.3 The regulations in the Agreement regarding applicable law and dispute resolution, shall apply correspondingly to this DPA.

****

By executing this DPA, the Parties agree to the terms of this DPA. This DPA and the Agreement may be executed in counterparts including facsimile, PDF and other electronic copies, each of which will be deemed an original and together will constitute one and the same agreement.

Annex 1

DESCRIPTION OF THE PROCESSING AND INSTRUCTIONS FROM THE DATA CONTROLLER

Purpose(s) for which the personal data is processed on behalf of the controller

The purpose of the processing is

1. to deliver telephony and communication services in accordance with the Agreement entered into by the Parties
2. to support the Service with which the customer is supplied
3. otherwise discharge responsibilities and Customer's instructions under the Agreement.

Duration of the processing

The term of the Agreement. Upon termination of the Agreement, Personal Data is deleted from active systems and is phased out from backups over time (subject to requirements to retain and delete data under applicable law). These backups have limited access, and Personal Data can remain for a maximum of two (2) years.

Categories of data subjects whose personal data is processed

End users – i.e. Customer's co-workers

The following types of Personal Data are processed:

- Name
- Email
- User ID
- Phone number
- IP address
- User-generated data, e.g. communication information such as call detail records, data consumption, video conference records, chat records
- Profile picture (optional, if uploaded by end users)
- Recordings (optional, set by administrator)
- User event logs for fulfilling support and maintenance services undertakings

Place of storage and processing of data

Telavox's storage and processing of data takes place within the EEA (except as applicable for optional services stated in Telavox Sub-Processor).

INSTRUCTIONS FROM THE DATA CONTROLLER CONCERNING THE PROCESSING OF PERSONAL DATA

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

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 ex- ample, certain Personal Data is registered with said operator.

  Personal Data may also be disclosed to other companies and authorities after the Customer 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.

Annex 2

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational security measures implemented by the data processor(s)

The Processor has undertaken the requisite technical and organisational measures in order to guarantee the integrity and confidentiality of Customer data.

Telavox reserves the right to revise these technical and organisational measures at any time, without notice, so long as any such revision will not reduce or weaken the protection provided for personal data that Telavox processes in providing its products and services.

Staff Confidentiality

The Processor has undertaken the requisite measures in order to guarantee that staff using the Customer's data 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
- Processor shall adhere to current policies and work procedures
- Continuous training and skill-enhancing measures

Physical security

The Processor ensures maintenance of an appropriate level of physical security in areas where the Customer'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 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 Customer. This may include:

- Appropriate firewall protection
- Audit logging for service monitoring
- Access control for service and systems
- Rights access 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

Management of Risk and IT Governance

The Processor ensures that a risk-based and appropriate level of governance is maintained. This may include:

- Conduct periodic reviews and assessments of risks, monitoring and maintaining of existing policies and procedures
- Periodic and effective reporting of information security conditions and compliance to senior internal management
- Maintaining a central IT Policy covering guidelines for information and cybersecurity topics

Customer's Security Responsibilities and Assessments

Without prejudice to Telavox's obligations under section 5.1-5.4, and elsewhere in the Agreement, Customer is responsible for its own technical and organisational measures, including without limitations storage of any copies of Customer Data outside Telavox or Telavox's Subprocessors' systems, securing the account authentication credentials, systems and devices Customer uses to access the service. or weaken the protection provided for personal data that Telavox processes in providing its products and services.