

Your continued use of Yeastar IPPBX means you are herein consenting to the following data procedures expressed within this agreement.

Yeastar S-Series VoIP PBX Data Processing Agreement

Your continued use of Yeastar S-Series VoIP PBX (“Services”) means you are herein consenting to the following data procedures expressed within this Data Processing Agreement (“DPA”).

The Data Controller (“Customer”) and the Data Processor (“Yeastar”) are hereinafter referred to as the Party or jointly the Parties.

1. DEFINITIONS

1.1 The terms used in this DPA 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 DPA may change during the term of the agreement. The above means that this DPA involves the following definitions:

Processing: the measure or combination of measures concerning Personal Data or sets of Personal Data, e.g. collection, registration, organization, 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 Law: the General Data Protection Regulation (EU) 2016/679 (‘GDPR’), and other regulations with the relevant implementation statutes and the regulations in this area applying at any given time. Non-European Data Protection Legislation may also apply to the processing of Customer Personal Data.

Data Controller: the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

Data Processor: the entity which processes Personal Data on behalf of the Controller.

Personal Data: any information relating to an identified or identifiable natural person.

Personal Data Breach: security incidents leading to unintentional or unlawful destruction, loss or alteration, or to unauthorized disclosure of or unauthorized 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 Data Processor that processes Personal Data on behalf of the Data Controller.

2. Background and Roles

2.1 **Parties' Roles.** Customer, as Data Controller, appoints Yeastar as a Data Processor to process the Personal Data on Customer's behalf. The processing the Data Processor will perform on behalf of the Data Controller shall be regulated by this DPA.

2.2 **Purpose Limitation.** Data Processor shall process the Personal Data for the purposes described in Annex A, except where otherwise required by applicable law. Any additional processing required by Data Controller outside of the scope of the DPA will require prior written agreement between the parties, including agreement on any additional fees that Data Controller may be required to pay.

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

3. Obligation of Data Processor

3.1 **Security.** Data Processor will maintain appropriate security measures to safeguard the security of Personal Data. Data Processor will maintain an information security and risk management program based on commercial best practices to preserve the confidentiality, integrity and accessibility of Personal Data with administrative, technical and physical measures conforming to generally recognized industry standards and practices. Data Processor shall implement appropriate technical and organizational measures to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

3.2 **Confidentiality.** Data Processor shall ensure that any personnel whom Data Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with

respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

3.3 Personal Data Breaches. Data Processor will notify the Data Controller as soon as practicable after it becomes aware of any of any Personal Data Breach affecting any Personal Data. At the Data Controller's request, Processor will promptly provide the Data Controller with all reasonable assistance necessary to enable the Data Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Data Controller is required to do so under the Data Protection Law.

3.4 Data Subject Requests. Data Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Data Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Data Processor, Data Processor will promptly inform Data Controller and will advise Data Subjects to submit their request to the Data Controller. Data Controller shall be solely responsible for responding to any Data Subjects' requests. Data Controller shall reimburse Data Processor for the costs arising from this assistance.

3.5 Sub-processors. Data Processor shall be entitled to engage Sub-processors to fulfil Data Processor's obligations only with Data Controller's written consent. The Data Processor shall inform the Data Controller of any intended changes concerning addition or replacement of any Sub-processors, and the Data Controller has the right to object to such changes. The Data Processor shall ensure that its data protection obligations set out in the DPA and in Applicable Data Protection Law are imposed to any Sub-processors by a written agreement. Any Sub-processor shall in particular provide sufficient guarantees to implement appropriate technical and organizational measures to comply with Applicable Data Protection Law, and provide the Data Controller and relevant supervisory authorities with access and information necessary to verify such compliance. The Data Processor shall remain fully liable to the Controller for the performance of any Sub-processor.

4. Data Controller Responsibility

Within the scope of the DPA and in its use of the services, Data Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Data Processor and the Processing of Personal Data. Customer, as Data Controller, shall be responsible for ensuring that:

4.1 It has complied, and will continue to comply, with all Applicable Data Protection Law, including in any instructions it issued to Yeastar under this DPA.

4.2 It has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Yeastar for processing in accordance with this DPA.

5. Validity

5.1 This DPA is valid until the Data Processor's processing of the Personal Data ceases.

5.2 Upon completion of processing, the Data Processor shall return the Personal Data to the 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.

Annex A Details of Processing

These instructions form an integral part of the DPA and shall be adhered to by the Data Processor in the processing of Personal Data, unless expressly state otherwise in the DPA. The Data Controller may unilaterally change these instructions at a later date by notifying the Data Processor of the change in writing.

Changes take effect no earlier than 3 calendar days after having been sent by the Data Controller. By accepting the DPA, the Data Controller Processor has confirmed the meaning of these instructions.

Purpose

The purpose of the processing is

- 1) to deliver telephony and communication Services
- 2) to support the Service with which the customer is supplied

Type of Processing

Registration of user data, storage of Personal Data, storage of use of the Services, statistical analyses, troubleshooting.

Type of Personal Data

The following types of Personal Data are processed:

Name

Password

Email

Phone number

IP address

User-generated content, e.g. call information

User behavior, system log for troubleshooting

The Data Controller and its users can upload Personal Data e.g. profile picture, phone number, address and further contact details. Upon uploading, the Data Controller approves the Data Processor's processing and storage of this information.

The Data Controller and its users can enable/disable certain features, e.g. LDAP, Call Recording, Remote Management. Upon enabling these features, the Data Controller approves the Data Processor's processing and storage of this information.

Duration of Processing

Processing lasts for as long as the Data Processor represents the Data Controller. Upon termination of the Services, Personal Data can be deleted by resetting the S-Series VoIP PBX to factory default.

Disclosure of Personal Data

Personal Data may be disclosed to:

Authorities

On request, and in accordance with the law and official decisions, the 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 Data Controller has given consent, and/or in order to discharge a specific part of the Service under an agreement.

I have read and agree to the above Agreement