DATA PROCESSING AGREEMENT (DPA) — VERSION 1.0 · 15.09.2026

1. Parties and Roles The Provider / processor is Simone Venneri, Föhrenweg 20, 5606 Dintikon, Switzerland, acting as an individual under the business name “Sympel Monitoring”. To the extent Sympel processes personal data on behalf of the Customer, the Provider acts as processor. Where the Customer acts as processor for a third party, Sympel acts as subprocessor. Processing for the Provider's own purposes, in particular contract administration, billing, security, abuse prevention and legal obligations, is described in the Privacy Policy.

2. Subject Matter, Duration, Nature and Purpose The subject matter is the technical provision of SaaS monitoring and operational intelligence for Yeastar environments during the contract term plus the agreed offboarding/retention period. Processing includes collecting/receiving, storing, structuring, retrieving, analysing, correlating, displaying, transmitting to approved subprocessors and controlled deletion. Purposes include PBX monitoring, incident correlation, trunk/provider health, Agent diagnostics, Media Path Diagnostics, location/ geodata functions, notifications, support, security and technical service delivery.

3. Data Subjects and Data Categories Data subjects may include Customer/MSP users, contacts, end-customer contacts and persons whose technical identifiers appear in operational/security data. Data categories include account/contact data, technical identifiers, IP addresses, hostnames, location/address data, PBX/trunk/provider metadata, Agent/network diagnostics, incident/audit data and communication metadata. Call content/ recordings, health/biometric data, data concerning criminal proceedings/sanctions and other specially sensitive/ special-category data are not intended for the standard service and must not be intentionally submitted without a separate written agreement.

4. Documented Instructions Initial activation and configuration of the service by the Customer constitutes a documented instruction to process the data described in this DPA for the stated purposes. Further instructions may be given through authorised use/configuration of the service or in text form. If Sympel considers an instruction unlawful, execution may be suspended and the Customer informed where legally permitted.

5. Customer Obligations The Customer warrants that it is authorised to transmit and process the data, provides required notices and has the necessary legal bases or authority to issue instructions. The Customer must not intentionally submit sensitive content excluded from the standard service.

6. Confidentiality and Security Persons authorised to access Customer Data are bound by confidentiality and receive access on a need-to-know/least-privilege basis. Sympel implements risk-appropriate technical and organisational measures according to the current TOM and will not materially reduce the agreed level of protection.

7. Subprocessors The Customer grants general authorisation for the subprocessors identified in the current Subprocessor List. Sympel will generally inform the Customer at least 14 days before the intended addition or replacement of any subprocessor that processes Customer Data. A shorter notice period is permitted only where compelling legal, security or operational reasons require an earlier change; in that case the Customer will be informed as early as reasonably possible. The Customer may raise reasoned data-protection objections within 14 days after notice. Sympel will seek a reasonable solution. If no reasonable solution is available and the change materially affects the service or the Customer's data-protection position, the Customer may terminate the affected service on 30 days' notice without a termination fee. Fees prepaid for the unused period of the affected service after termination takes effect will be refunded pro rata. Subprocessors are contractually required to provide an appropriate level of protection meeting applicable requirements.

8. International Transfers Processing locations, possible access and transfer mechanisms are documented in the Subprocessor List. For recipients in countries without recognised adequate data protection, recognised standard contractual clauses with Swiss adaptations, applicable Data Privacy Framework certifications or other

legally permitted safeguards are used where required. No region is represented as EU-only unless guaranteed by the concrete service architecture.

9. Assistance Taking into account the nature of processing, Sympel will reasonably assist the Customer with data-subject rights, deletion, restriction, data provision, security incidents, data-protection impact assessments and supervisory-authority requests insofar as they concern data processed by Sympel.

10. Personal Data Breaches Sympel will inform the Customer without undue delay and no later than 48 hours after confirmed awareness of a relevant personal-data breach affecting entrusted data. The notification will contain the information available at that time; further findings may be provided subsequently.

11. Deletion, Return and Retention Before expiry of the offboarding period, the Customer may request, where technically available and subject to third-party rights, an export of its organisation-related operational and monitoring data in a commonly used machine-readable or otherwise reasonably readable format. Upon reasoned request, after completion of the controlled deletion process Sympel will confirm in text form the deletion or anonymisation of productive Customer Data; records subject to legal retention and data remaining in protected backups until expiry of the applicable provider lifecycle are excluded.

Following termination of a contract/pilot, a 30-day offboarding and recovery period generally applies. After that period, productive organisation-related operational and monitoring data is deleted or anonymised through the controlled deletion process unless a legal hold applies. Contract, invoice, payment, security, audit and acceptance evidence is retained separately and only for as long as required for legal obligations, security, establishment/defence of claims or proof of contract conclusion. Documented internal retention rules apply to each category. Backups remain protected until expiry of the technically applicable provider backup lifecycle and are not further processed for ordinary customer operations; no shorter specific backup-deletion deadline is promised while the provider lifecycle is not contractually documented.

12. Evidence and Audits Sympel will provide reasonable information demonstrating compliance with this DPA. Audits should primarily be satisfied through TOM, security documentation, certifications or independent reports. A residual audit right remains in case of a relevant privacy/security incident, a justified regulatory requirement, or where existing evidence is objectively insufficient. Audits require reasonable prior notice, confidentiality and safeguards against disproportionate impact on other customers or security.

13. Duration and Precedence This DPA applies for the duration of processing and to surviving obligations. In case of inconsistency between the German and English versions, the German version prevails unless expressly agreed otherwise.

ANNEX 1 — PROCESSING DESCRIPTION Subject matter: SaaS monitoring and operational intelligence for Yeastar environments. Duration: Contract/pilot term plus approved offboarding/retention period. Frequency: Continuous/periodic according to monitoring configuration. Data subjects: Customer/MSP users, contacts, end-customer contacts and technical identifiers associated with managed systems. Data: Account/contact data, technical identifiers, IP/hostname, location/address data, PBX/trunk/provider metadata, Agent/network diagnostics, incident/audit data and communication metadata. Special data: Not intended as a standard service category; excluded sensitive content only under a separate written agreement.