AUFTRAGSBEARBEITUNGSVEREINBARUNG (AVV/DPA) — VERSION 1.0 · 15.09.2026

1. Parteien und Rollen Anbieter / Auftragsbearbeiter ist Simone Venneri, Föhrenweg 20, 5606 Dintikon, Schweiz, als Einzelperson handelnd unter der Geschäftsbezeichnung „Sympel Monitoring“. Soweit Sympel Personendaten im Auftrag des Kunden bearbeitet, handelt der Anbieter als Auftragsbearbeiter. Handelt der Kunde als Auftragsbearbeiter eines Dritten, handelt Sympel als Unterauftragsbearbeiter. Eigene Bearbeitungszwecke des Anbieters, insbesondere Vertragsverwaltung, Abrechnung, Sicherheit, Missbrauchsprävention und gesetzliche Pflichten, werden in der Datenschutzerklärung beschrieben.

2. Gegenstand, Dauer, Art und Zweck Gegenstand ist die technische Bereitstellung von SaaS Monitoring und Operational Intelligence für Yeastar-Umgebungen während der Vertragsdauer zuzüglich der vereinbarten Offboarding-/Retention-Periode. Die Bearbeitung umfasst Erheben/Empfangen, Speichern, Strukturieren, Abfragen, Analysieren, Korrelieren, Anzeigen, Übermitteln an genehmigte Unterauftragsbearbeiter sowie kontrolliertes Löschen. Zwecke sind PBX Monitoring, Incident Correlation, Trunk-/Provider Health, Agent Diagnostics, Media Path Diagnostics, Standort-/Geodatenfunktionen, Benachrichtigungen, Support, Sicherheit und technische Bereitstellung.

3. Betroffene Personen und Datenkategorien Betroffene können Kunden-/MSP-Benutzer, Ansprechpartner, Endkunden-Kontakte und Personen sein, deren technische Identifikatoren in Betriebs-/Sicherheitsdaten erscheinen. Datenkategorien: Account-/Kontaktdaten, technische Identifikatoren, IP-Adressen, Hostnamen, Standort-/Adressdaten, PBX-/Trunk-/Provider-Metadaten, Agent-/Netzwerkdiagnostik, Incident-/Auditdaten und Kommunikationsmetadaten. Gesprächsinhalte/-aufzeichnungen, Gesundheits-/biometrische Daten, Daten über strafrechtliche Verfolgungen/Sanktionen oder andere besonders schützenswerte/besondere Kategorien sind nicht für den Standarddienst vorgesehen und dürfen ohne separate schriftliche Vereinbarung nicht absichtlich übermittelt werden.

4. Dokumentierte Weisungen Die erstmalige Aktivierung und Konfiguration des Dienstes durch den Kunden gilt als dokumentierte Weisung zur Bearbeitung der in diesem DPA beschriebenen Daten für die genannten Zwecke. Weitere Weisungen können durch berechtigte Nutzung/Konfiguration des Dienstes oder in Textform erteilt werden. Hält Sympel eine Weisung für rechtswidrig, darf die Ausführung ausgesetzt und der Kunde informiert werden, soweit gesetzlich zulässig.

5. Pflichten des Kunden Der Kunde gewährleistet, dass er zur Übermittlung und Bearbeitung der Daten berechtigt ist, erforderliche Informationen erteilt und Rechtsgrundlagen bzw. Weisungsbefugnisse besitzt. Der Kunde darf keine für den Standarddienst ausgeschlossenen sensiblen Inhalte absichtlich übermitteln.

6. Vertraulichkeit und Sicherheit Zugriffsberechtigte Personen sind auf Vertraulichkeit verpflichtet und erhalten Zugriff nach Need-to-know/Least-Privilege. Sympel implementiert risikoadäquate technische und organisatorische Massnahmen gemäss dem aktuellen TOM-Anhang und reduziert das vereinbarte Schutzniveau nicht wesentlich.

7. Unterauftragsbearbeiter Der Kunde erteilt eine allgemeine Genehmigung für die in der aktuellen Subprocessor List bezeichneten Unterauftragsbearbeiter. Sympel informiert den Kunden grundsätzlich mindestens 14 Tage vor der beabsichtigten Hinzunahme oder Ersetzung jedes Unterauftragsbearbeiters, der Kundendaten bearbeitet. Eine kürzere Frist ist nur zulässig, wenn zwingende rechtliche, sicherheitsbezogene oder betriebliche Gründe eine frühere Änderung erfordern; der Kunde wird dann so früh wie vernünftigerweise möglich informiert. Der Kunde kann innerhalb von 14 Tagen nach Mitteilung begründete datenschutzrechtliche Einwände erheben. Sympel bemüht sich um eine zumutbare Lösung. Ist keine zumutbare Lösung verfügbar und beeinträchtigt die Änderung den Dienst oder die Datenschutzposition des Kunden wesentlich, kann der Kunde den betroffenen Dienst mit einer Frist von 30 Tagen ohne Kündigungsgebühr kündigen. Bereits im Voraus

bezahlte Vergütungen für den nach Wirksamwerden der Kündigung nicht mehr genutzten Zeitraum des betroffenen Dienstes werden anteilig zurückerstattet. Unterauftragsbearbeiter werden vertraglich zu einem angemessenen, den anwendbaren Anforderungen entsprechenden Schutzniveau verpflichtet.

8. Auslandbekanntgaben Verarbeitungsstandorte, mögliche Zugriffe und Transfermechanismen werden in der Subprocessor List dokumentiert. Für Empfänger in Staaten ohne anerkannt angemessenes Datenschutzniveau werden, soweit erforderlich, anerkannte Standardvertragsklauseln mit schweizerischen Anpassungen, anwendbare Data-Privacy-Framework-Zertifizierungen oder andere gesetzlich zulässige Garantien verwendet. Keine Region wird als EU-only zugesichert, sofern dies die konkrete Servicearchitektur nicht garantiert.

9. Unterstützung Unter Berücksichtigung der Art der Bearbeitung unterstützt Sympel den Kunden angemessen bei Betroffenenrechten, Löschung, Einschränkung, Datenherausgabe, Sicherheitsvorfällen, Datenschutz-Folgenabschätzungen und Behördenanfragen, soweit dies die von Sympel bearbeiteten Daten betrifft.

10. Datenschutzvorfälle Sympel informiert den Kunden ohne unangemessene Verzögerung, spätestens innerhalb von 48 Stunden nach bestätigter Kenntnis eines relevanten Datenschutzvorfalls, der Auftragsdaten betrifft. Die Mitteilung enthält die zu diesem Zeitpunkt verfügbaren Informationen; weitere Erkenntnisse können nachgereicht werden.

11. Löschung, Rückgabe und Retention Vor Ablauf der Offboarding-Periode kann der Kunde, soweit technisch verfügbar und unter Wahrung der Rechte Dritter, einen Export seiner organisationsbezogenen Betriebs- und Monitoring-Daten in einem gängigen maschinenlesbaren oder anderweitig angemessen lesbaren Format anfordern. Auf begründete Anfrage bestätigt Sympel nach Abschluss des kontrollierten Löschprozesses die Löschung oder Anonymisierung der produktiven Kundendaten in Textform; gesetzlich aufzubewahrende Nachweise und Daten in geschützten Backups bis zum Ablauf des anwendbaren Provider-Lebenszyklus bleiben hiervon ausgenommen.

Nach Vertrags-/Pilotende gilt grundsätzlich eine 30-tägige Offboarding- und Wiederherstellungsperiode. Danach werden produktive organisationsbezogene Betriebs- und Monitoring-Daten im kontrollierten Löschprozess gelöscht oder anonymisiert, soweit keine rechtliche Sperre entgegensteht. Vertrags-, Rechnungs-, Zahlungs-, Sicherheits-, Audit- und Akzeptanznachweise werden getrennt und nur solange aufbewahrt, wie dies für gesetzliche Pflichten, Sicherheit, die Durchsetzung/Abwehr von Ansprüchen oder den Nachweis eines Vertragsschlusses erforderlich ist. Für jede Kategorie gelten dokumentierte interne Aufbewahrungsregeln. Sicherungskopien verbleiben bis zum Ablauf des technisch geltenden Provider-Backup-Lebenszyklus geschützt und werden nicht für normalen Kundenbetrieb weiterverarbeitet; ein kürzerer konkreter Backup-Löschtermin wird nicht zugesichert, solange der Provider-Lebenszyklus nicht verbindlich dokumentiert ist.

12. Nachweise und Audits Sympel stellt angemessene Informationen zur Einhaltung dieses DPA zur Verfügung. Audits sollen vorrangig durch TOM, Sicherheitsdokumentation, Zertifizierungen oder unabhängige Berichte erfüllt werden. Ein weitergehendes Auditrecht bleibt bei einem relevanten Datenschutz-/Sicherheitsvorfall, einer begründeten regulatorischen Verpflichtung oder wenn vorhandene Nachweise objektiv nicht ausreichen, bestehen. Audits erfolgen mit angemessener Vorankündigung, unter Vertraulichkeit und ohne unverhältnismässige Beeinträchtigung anderer Kunden oder der Sicherheit.

13. Dauer und Vorrang Dieses DPA gilt für die Dauer der Bearbeitung und für fortbestehende Pflichten. Bei Widersprüchen zwischen deutscher und englischer Fassung ist die deutsche Fassung massgebend, sofern nicht ausdrücklich anders vereinbart.

ANLAGE 1 — BEARBEITUNGSBESCHREIBUNG Gegenstand: SaaS Monitoring und Operational Intelligence für Yeastar-Umgebungen. Dauer: Vertrags-/Pilotdauer plus genehmigte Offboarding-/Retention-Periode. Häufigkeit: kontinuierlich/periodisch entsprechend der Monitoring-Konfiguration. Betroffene: Kunden-/MSP-

Benutzer, Ansprechpartner, Endkunden-Kontakte und technische Identifikatoren verwalteter Systeme. Daten: Account-/Kontaktdaten, technische Identifikatoren, IP/Hostname, Standort-/Adressdaten, PBX-/Trunk-/Provider-Metadaten, Agent-/Netzwerkdiagnostik, Incident-/Audit- und Kommunikationsmetadaten. Besondere Daten: nicht als Standard-Servicekategorie vorgesehen; ausgeschlossene sensible Inhalte nur nach separater schriftlicher Vereinbarung.