Anlage B.

Vereinbarung zur Auftragsverarbeitung

Fassung 1.2 · 4. November 2026

1. Gegenstand, Rollen und Dauer

1.1 Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten durch die Consoper UG (haftungsbeschränkt), Am Markt 1, 28195 Bremen („Consoper“), im Auftrag des Kunden bei der Bereitstellung von AuroNeo Flex nach Art. 28 DSGVO. Der Kunde ist Verantwortlicher, Consoper ist Auftragsverarbeiter. Begriffe haben die Bedeutung der DSGVO und der AGB.

1.2 Die Vereinbarung gilt für die Dauer des Vertrags einschließlich der Abrufzeit nach Ziffer 13.8 der AGB und bis zur Löschung nach Ziffer 9. Sie wird bei der Online-Bestellung durch die ausdrückliche Erklärung des Kunden elektronisch geschlossen (Art. 28 Abs. 9 DSGVO), beim persönlichen Angebot mit dessen Annahme. Für einen Testzugang mit eigenen personenbezogenen Daten gilt sie vor Beginn der Verarbeitung (Ziffer 15.2 der AGB).

1.3 Nicht Gegenstand dieser Vereinbarung ist die Verarbeitung der Vertrags-, Abrechnungs- und Kontaktdaten des Kunden durch Consoper als eigener Verantwortlicher; dafür gelten die Datenschutzhinweise von Consoper.

---

2. Art und Zweck der Verarbeitung

2.1 Consoper verarbeitet die Daten ausschließlich, um AuroNeo Flex nach dem Vertrag bereitzustellen: Speichern, Anzeigen, Berechnen und Auswerten der vom Kunden eingegebenen und importierten Daten, Erzeugen von Exporten, Datensicherung und Wiederherstellung, Bearbeitung von Supportanfragen sowie Rückgabe und Löschung. Eine Nutzung für eigene Zwecke, für Werbung, zum Weiterverkauf oder zum Training von KI-Modellen findet nicht statt (Ziffer 5.4 der AGB).

---

3. Betroffene Personen und Datenarten

3.1 Betroffen sind insbesondere: Beschäftigte des Kunden einschließlich geringfügig und kurzfristig Beschäftigter, Honorarkräfte, Übungsleiter und Ehrenamtliche; Benutzer der Anwendung; Zahlungsempfänger und sonstige Gegenparteien aus Bankumsätzen, Kasse und Rechnungen; Ansprechpartner und Leitungen von Kostenstellen.

3.2 Verarbeitet werden insbesondere:

- Personaldaten: Name, Personalnummer, Beginn, Ende und Befristung der Beschäftigung, Art der Beschäftigung, vertragliche Stunden und deren Verteilung auf Kostenstellen, Tarifwerk,

Entgeltgruppe und Stufe, Gehalt, Zulagen, Jahressonderzahlung, Arbeitgeberanteile zur Sozialversicherung, Zusatzversorgung und Berufsgenossenschaft, bei Minijobs Angaben zur Pauschalsteuer und zur Art der Krankenversicherung, Honorarart und Honorar, freie Notizen;

- Bank- und Buchungsdaten: eigene Bankkonten des Kunden (IBAN, BIC, Kontoinhaber), Umsätze mit Verwendungszweck, Gegenkonto und Empfänger, Buchungen, Kassenbuchungen, Rechnungsfreigaben mit Empfänger und Empfänger-IBAN;
- Belege und Dokumente: hochgeladene Dateien mit Dateiname und Inhalt;
- Benutzerdaten: E-Mail-Adresse, Anzeigename, Rolle, Rechte, Anmelde- und Sicherheitsdaten (Passwort nur als Hashwert, Zwei-Faktor-Geheimnis verschlüsselt);
- Protokoll- und Supportdaten: Änderungsprotokoll mit Benutzerkennung, E-Mail-Adresse, IP-Adresse und Zeitpunkt; Supportanfragen mit Name, E-Mail-Adresse, Rolle, Seite, Browser und Freitext.

3.3 Die Anwendung sieht keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) vor, etwa Gesundheits- oder Religionsangaben. Sie können nur über Freitexte, Verwendungszwecke oder Belege hineingelangen. Der Kunde vermeidet das, soweit es für seinen Zweck nicht erforderlich ist; Patientendokumentation, Befunde und Sozialdaten verarbeitet er nur nach vorheriger Vereinbarung (Ziffer 5.3 der AGB).

---

4. Weisungen

4.1 Consoper verarbeitet die Daten nur auf dokumentierte Weisung des Kunden. Die Weisungen ergeben sich aus dem Vertrag und aus der Nutzung der Funktionen der Anwendung durch die Benutzer des Kunden. Weitere Weisungen erteilt der Kunde in Textform an support@auroneo.de.

4.2 Ist Consoper der Auffassung, dass eine Weisung gegen Datenschutzrecht verstößt, weist sie den Kunden unverzüglich darauf hin (Art. 28 Abs. 3 Satz 3 DSGVO) und darf die Ausführung bis zur Klärung aussetzen. Ist Consoper durch Unionsrecht oder das Recht eines Mitgliedstaats zu einer anderen Verarbeitung verpflichtet, teilt sie dies dem Kunden vorher mit, soweit das Recht dies nicht verbietet.

---

5. Pflichten von Consoper

5.1 Personen, die bei Consoper Zugriff auf die Daten haben, sind zur Vertraulichkeit verpflichtet. Zugriff erhalten nur Personen, die ihn für Betrieb, Sicherung oder Support benötigen, und nur im erforderlichen Umfang.

5.2 Consoper trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die im Anhang dieser Anlage beschrieben sind. Sie darf die Maßnahmen an den Stand der Technik anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen teilt sie dem Kunden in Textform mit.

5.3 Consoper unterstützt den Kunden bei der Erfüllung der Rechte betroffener Personen. Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragung kann der Kunde mit den Funktionen der Anwendung und den Exporten nach Anlage C selbst erledigen. Wendet sich eine betroffene Person unmittelbar an Consoper, leitet Consoper die Anfrage unverzüglich an den Kunden weiter.

5.4 Consoper unterstützt den Kunden angemessen bei seinen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere mit den Angaben dieser Anlage für eine Datenschutz-Folgenabschätzung.

5.5 Consoper meldet dem Kunden eine Verletzung des Schutzes der im Auftrag verarbeiteten Daten unverzüglich, nachdem sie ihr bekannt geworden ist, an die im Vertrag benannte Kontaktadresse. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben werden nachgereicht. Consoper ergreift unverzüglich Maßnahmen zur Eindämmung und unterstützt den Kunden bei Meldung und Benachrichtigung.

5.6 Ansprechpartner für den Datenschutz bei Consoper ist erreichbar unter support@auroneo.de.

---

6. Pflichten des Kunden

6.1 Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und die Information der betroffenen Personen verantwortlich. Er legt Benutzerkonten und Rechte fest und beschränkt sie auf das erforderliche Maß (Ziffer 4.2 der AGB), insbesondere das Recht, Gehaltsdaten zu sehen. Stellt er Fehler oder Unregelmäßigkeiten bei der Verarbeitung fest, informiert er Consoper unverzüglich.

---

7. Weitere Auftragsverarbeiter

7.1 Der Kunde genehmigt den Einsatz folgender weiterer Auftragsverarbeiter:

- **Hetzner Online GmbH**, Industriestraße 25, 91710 Gunzenhausen: Betrieb des Servers und des getrennten Sicherungsspeichers, beide in Falkenstein (Deutschland);
- **Brevo GmbH**, Köpenicker Straße 126, 10179 Berlin: Versand der System-E-Mails (Bestätigungen, Einladungen, Links zum Zurücksetzen des Passworts, Benachrichtigungen über Supportanfragen); verarbeitet werden E-Mail-Adressen, Namen und der Inhalt dieser E-Mails;
- **netcup GmbH**, Emmy-Noether-Straße 10, 76131 Karlsruhe (Deutschland): E-Mail-Postfach support@auroneo.de, in dem Supportanfragen und Benachrichtigungen eingehen.

7.2 Keine weiteren Auftragsverarbeiter im Sinne dieser Vereinbarung sind Dienste, die keine Kundendaten erhalten, insbesondere die Verfügbarkeitsprüfung, die nur einen öffentlichen Statusendpunkt abruft, und die Ausgabe von TLS-Zertifikaten. Ebenso wenig Lexware Office, SepaHeld und GoCardless: Sie erhalten nur die Vertrags- und Abrechnungsdaten des Kunden als Vertragspartner von Consoper (Ziffer 1.3), keine in AuroNeo Flex gespeicherten Daten.

7.3 Consoper verpflichtet weitere Auftragsverarbeiter vertraglich auf Datenschutzpflichten, die dieser Vereinbarung entsprechen (Art. 28 Abs. 4 DSGVO). Den Einsatz eines neuen oder den Austausch eines weiteren Auftragsverarbeiters teilt Consoper dem Kunden mindestens vier Wochen vorher in Textform mit. Der Kunde kann innerhalb von zwei Wochen nach Zugang aus wichtigem datenschutzrechtlichem Grund widersprechen. Einigen sich die Parteien nicht, kann jede Partei den Vertrag zum Zeitpunkt des Wechsels außerordentlich kündigen; Ziffer 13 der AGB bleibt unberührt.

7.4 Consoper selbst verarbeitet Kundendaten nicht außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums. Setzen die weiteren Auftragsverarbeiter nach Ziffer 7.1 für unterstützende Leistungen eigene Dienstleister außerhalb des Europäischen Wirtschaftsraums ein,

geschieht dies nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage eines Angemessenheitsbeschlusses oder von Standardvertragsklauseln. Auskunft über die geltenden Garantien erteilt Consoper auf Anfrage.

8. Nachweise und Kontrollen

8.1 Consoper stellt dem Kunden auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung erforderlich sind. Der Kunde kann Überprüfungen einschließlich Inspektionen selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen, nach Anmeldung mit angemessener Frist, in der Regel zwei Wochen, während der üblichen Geschäftszeiten und ohne Störung des Betriebs und anderer Mandanten. Für das Rechenzentrum genügen die Nachweise des Rechenzentrumsbetreibers.

9. Rückgabe und Löschung

9.1 Die Rückgabe der Daten erfolgt über den Export nach Anlage C, während der Vertragslaufzeit jederzeit und nach dem Vertragsende innerhalb der Abrufzeit von 30 Kalendertagen (Ziffer 13.8 der AGB).

9.2 Nach Ablauf der Abrufzeit löscht Consoper die Daten des Mandanten im laufenden System unverzüglich, spätestens innerhalb von 14 Kalendertagen, sofern der Kunde keine frühere Löschung angewiesen hat (Ziffer 14 der AGB).

9.3 In den verschlüsselten Sicherungen nach Anlage A Ziffer 8.2 sind gelöschte Daten noch bis zum Ablauf der Sicherungsstände enthalten, längstens 60 Kalendertage nach der Löschung im laufenden System. Sie werden in dieser Zeit nicht verwendet. Wird ein Sicherungsstand wiederhergestellt, wendet Consoper die zwischenzeitlichen Löschungen erneut an.

9.4 Einträge des Änderungs- und Sicherheitsprotokolls mit Bezug zum Mandanten bewahrt Consoper zum Nachweis der ordnungsgemäßen Verarbeitung bis zu drei Jahre nach ihrer Entstehung auf. Sie enthalten keine Gehalts- und Personalinhalte, werden zu keinem anderen Zweck verwendet und danach gelöscht. Vertrags- und Abrechnungsunterlagen von Consoper werden nach Ziffer 14.2 der AGB getrennt aufbewahrt.

9.5 Auf Anfrage bestätigt Consoper die Löschung in Textform mit Datum (Löschnachweis).

10. Schlussbestimmungen

10.1 Für Fragen des Datenschutzes geht diese Vereinbarung den übrigen Vertragsbestandteilen vor. Für die Haftung gelten Art. 82 DSGVO und die Ziffern der AGB zur Haftung. Änderungen bedürfen der Textform.

Anhang: Technische und organisatorische Maßnahmen

T.1 Zutritt und Zugang zum Server. Der Server steht im Rechenzentrum Falkenstein der Hetzner Online GmbH mit Zutrittskontrolle durch den Rechenzentrumsbetreiber; Consoper hat keinen physischen Zugang. Administrativer Zugang ist nur per SSH mit Schlüssel möglich, eine Anmeldung mit Passwort ist abgeschaltet. Zugang haben nur von Consoper benannte Administratoren.

T.2 Zugang zur Anwendung. Persönliche Benutzerkonten; Passwörter mit mindestens 10 Zeichen, Abgleich mit einer Liste bekannter Passwörter, gespeichert nur als BCrypt-Hashwert; Zwei-Faktor-Anmeldung mit Authenticator-App für Administratoren und Betreiberkonten verpflichtend; Bestätigung der E-Mail-Adresse; Sperre nach wiederholten Fehlversuchen; Sitzungsende nach 20 Minuten ohne Aktivität und spätestens nach 12 Stunden; Begrenzung der Anfragen je Benutzer, Mandant und Absender.

T.3 Zugriffsrechte. Rollenmodell (Administrator, Projektleitung, Sachbearbeitung mit Rechten je Kostenstelle, Geschäftsführung und Lesezugriff mit reinen Leserechten); gesondertes Recht zum Sehen von Gehaltsdaten, standardmäßig ausgeschaltet; Exporte nur für berechtigte Rollen.

T.4 Trennung. Logische Mandantentrennung: Jeder Datenbankzugriff ist automatisch auf den Mandanten des Benutzers beschränkt, und ein Schreibschutz verhindert das Speichern von Daten in einen fremden Mandanten. Entwicklung, Tests und Vorführungen verwenden nur erfundene Daten.

T.5 Verschlüsselung. Übertragung ausschließlich verschlüsselt (HTTPS mit TLS, HSTS); E-Mail-Versand mit TLS. Datenbank, Belegdateien und Protokolle liegen in einem verschlüsselten Speicherbereich des Servers; der Schlüssel wird nicht auf dem Server gespeichert. Sicherungen werden vor der Übertragung verschlüsselt. Zwei-Faktor-Geheimnisse sind zusätzlich verschlüsselt gespeichert.

T.6 Datenminimierung in Protokollen. Betriebsprotokolle enthalten keine Namen, Gehälter oder Dateinamen und werden höchstens 14 Tage aufbewahrt. Deaktivierte Benutzerkonten werden nach sechs Monaten, Rohinhalte abgewiesener Importzeilen nach 90 Tagen bereinigt.

T.7 Eingabe- und Weitergabekontrolle. Ein Änderungsprotokoll hält fachlich relevante Änderungen mit Benutzer und Zeitpunkt fest. Exporte werden über verschlüsselte Verbindungen ausgeliefert; das Mandantenarchiv enthält Prüfsummen aller Dateien.

T.8 Schutz vor Schadsoftware. Hochgeladene Dateien werden auf dem Server mit einem Virenscanner geprüft; ist der Scanner nicht verfügbar, werden Uploads gesperrt.

T.9 Verfügbarkeit und Wiederherstellung. Tägliche verschlüsselte Sicherung von Datenbank, Belegdateien und Konfiguration auf einem getrennten Speicher; zusätzliche Sicherung vor Änderungen der Datenbankstruktur; wöchentliche Prüfung der Sicherungsdaten; regelmäßige Wiederherstellungsproben; automatische Überwachung der Erreichbarkeit alle fünf Minuten und Alarm bei einer Sicherung, die älter als 30 Stunden ist.

T.10 Regelmäßige Überprüfung. Vor der Auslieferung von Änderungen laufen automatisierte Tests, darunter Prüfungen der Mandantentrennung und der Berechtigungen. Die Anwendung wird mit einem dynamischen Sicherheitsscanner geprüft und die verwendeten Software-Abbilder auf bekannte

Schwachstellen. Für Sicherheitsvorfälle besteht ein dokumentierter Ablauf (Sperren, Widerrufen, Wiederherstellen, Nachweisen).