Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) · Thelixis e.U. · Stand: Juni 2026 · Version 1.0

Parteien

Auftragsverarbeiter (Anbieter):
Thelixis e.U.
Inhaberin: Kristina Momirovic
Hildebrandgasse 39, 1180 Wien, Österreich
FN 682107z · UID: ATU68027725 · office@iia-analysis.at

Verantwortlicher (Kunde):
Name/Firma: _____
Adresse: _____
E-Mail: _____
(nachfolgend „Verantwortlicher“)

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

1.1 Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Nutzung der SaaS-Plattform Thelixis e.U.

1.2 Art der Verarbeitung: Erhebung, Speicherung, Auswertung, Übermittlung und Löschung personenbezogener Daten gemäß Weisung des Verantwortlichen.

1.3 Zweck der Verarbeitung: Bereitstellung der gebuchten SaaS-Funktionen (Rechnungsanalyse, Vertragsübersicht, KI-gestützte Auswertung, Reporting, Benutzerverwaltung).

1.4 Dauer: Die Verarbeitung erfolgt für die Laufzeit des zugrundeliegenden Hauptvertrages (Nutzungsvertrag Thelixis e.U.). Nach Vertragsende gelten die Regelungen in § 8.

§ 2 Kategorien personenbezogener Daten und betroffene Personen

2.1 Kategorien personenbezogener Daten:

– Kontaktdaten (Name, E-Mail, Telefon) von Benutzern und Ansprechpartnern

– Telekommunikationsrechnungsdaten (Rufnummern, Vertragsdetails, Verbrauchsdaten)

– Zugangsdaten (Benutzername, verschlüsseltes Passwort, Session-Token)

– KI-Analyseeingaben und -ergebnisse (Rechnungstexte, Auswertungen)

– Log-Daten (Zeitstempel, IP-Adressen, Aktivitätsprotokolle)

2.2 Kategorien betroffener Personen: Mitarbeiterinnen und Mitarbeiter des Verantwortlichen, Kunden des Verantwortlichen soweit in Rechnungsdaten enthalten.

§ 3 Weisungsbindung

3.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet.

3.2 Weisungen sind schriftlich (auch per E-Mail) zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

3.3 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich.

§ 4 Vertraulichkeit

4.1 Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 5 Technische und organisatorische Maßnahmen (TOMs)

5.1 Der Auftragsverarbeiter trifft alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO. Konkret umgesetzte Maßnahmen umfassen insbesondere:

– Verschlüsselung der Datenübertragung (TLS 1.2/1.3)

– Verschlüsselung gespeicherter Passwörter (bcrypt)

– Zugriffskontrolle: rollenbasiertes Berechtigungskonzept, Mandantentrennung

– Pseudonymisierung: Session-IDs statt Klarnamen in Telemetriedaten

– Protokollierung: Zugriffsprotokoll, Fehlermeldungen (90 Tage Aufbewahrung)

– Löschkonzept: automatisierte Löschung nach definierten Fristen

– Subprozessor-Kontrolle: AVVs mit allen Unterauftragsverarbeitern

5.2 Der Auftragsverarbeiter ist berechtigt, die TOMs an den aktuellen Stand der Technik anzupassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Verantwortlichen vorab mitzuteilen.

§ 6 Einsatz von Unterauftragsverarbeitern (Subprozessoren)

6.1 Der Verantwortliche erteilt hiermit die allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern gemäß der nachfolgenden Liste:

– Render Services Inc. (USA) – Hosting/Infrastruktur – Rechtsgrundlage: EU-Standardvertragsklauseln (SCCs)

– Amazon Web Services EMEA SARL (Luxemburg, EU) – KI-Analyse via AWS Bedrock (eu-central-1 Frankfurt)

– Brevo SAS / Sendinblue (Frankreich, EU) – Transaktionale E-Mails

– Stripe Payments Europe Ltd. (Irland, EU) – Zahlungsabwicklung

– Cloudflare Inc. (USA) – DDoS-Schutz, Bot-Abwehr (Turnstile) – Rechtsgrundlage: SCCs

6.2 Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzufügung/Ersetzung) mit angemessener Vorlaufzeit. Der Verantwortliche hat das Recht, Einwände zu erheben.

6.3 Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeiter denselben Datenschutzpflichten unterliegen wie in diesem Vertrag vereinbart.

§ 7 Unterstützung bei Betroffenenrechten und Datensicherheit

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung von Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit)

durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist.

7.2 Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten (Datenpannen) unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntnisnahme, an den Verantwortlichen unter office@iia-analysis.at.

7.3 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Durchführung von Datenschutz-Folgenabschätzungen (DSFA) gemäß Art. 35 DSGVO, soweit erforderlich.

§ 8 Löschung und Rückgabe nach Auftragsende

8.1 Nach Beendigung des Hauptvertrages werden alle personenbezogenen Daten des Verantwortlichen auf dessen Wahl entweder zurückgegeben (Export als CSV/JSON) oder vollständig gelöscht. Die Löschung erfolgt innerhalb von 30 Tagen nach Vertragsende.

8.2 Soweit eine gesetzliche Aufbewahrungspflicht besteht (insb. § 132 BAO – 7 Jahre), verbleibt der Auftragsverarbeiter in dieser Pflicht, bis die Frist abgelaufen ist.

8.3 Auf Wunsch des Verantwortlichen stellt der Auftragsverarbeiter eine schriftliche Bestätigung der Löschung aus.

§ 9 Kontroll- und Prüfrechte

9.1 Der Verantwortliche hat das Recht, die Einhaltung dieses Vertrages und der anwendbaren Datenschutzvorschriften durch den Auftragsverarbeiter zu überprüfen. Prüfungen sind mit angemessener Vorlaufzeit (mindestens 14 Tage) schriftlich anzukündigen.

9.2 Der Auftragsverarbeiter stellt dem Verantwortlichen alle zur Nachweisführung erforderlichen Informationen zur Verfügung und ermöglicht Audits, die vom Verantwortlichen oder einem beauftragten Prüfer durchgeführt werden.

9.3 Alternativ kann der Auftragsverarbeiter aktuelle Zertifizierungen (ISO 27001 o.ä.) oder Prüfberichte vorlegen, die als gleichwertig anerkannt werden.

§ 10 Haftung

10.1 Für Schäden, die dem Verantwortlichen aufgrund eines Verstoßes des Auftragsverarbeiters gegen diesen Vertrag entstehen, haftet der Auftragsverarbeiter nach den allgemeinen gesetzlichen Haftungsregeln.

10.2 Der Auftragsverarbeiter haftet nicht für Schäden, die durch nicht autorisierte Weisungen des Verantwortlichen oder durch Verstöße des Verantwortlichen gegen die DSGVO entstehen.

§ 11 Schlussbestimmungen

11.1 Dieser Vertrag unterliegt österreichischem Recht. Gerichtsstand ist Wien.

11.2 Änderungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

11.3 Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

11.4 Dieser Vertrag tritt mit Unterzeichnung beider Parteien in Kraft und gilt für die Dauer des Hauptvertrages.

Unterschriften:

_____
Auftragsverarbeiter: Thelixis e.U.
Kristina Momirovic, Wien, Datum: _____

_____
Verantwortlicher: _____
Name/Funktion: _____, Datum: _____