

Vertrag zur Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordnung (DSGVO) · Fassung vom 24. September 2026

Verantwortliche/r (Auftraggeber)

Name / Praxis: _____

Anschrift: _____

E-Mail (Kosmogramm-Konto): _____

Auftragsverarbeiter (Auftragnehmer)

DEFI PIONEER LLC (Discovery Engine For Innovation),
handelnd unter dem Namen AI Pioneer
7901 4th St N, Ste 300, St. Petersburg, FL 33702, USA

Zustelladresse: c/o COCENTER, Koppoldstr. 1,
86551 Aichach

vertreten durch Sebastian Schenkyr · ai-pioneer@mail.de

EU-Vertreter (Art. 27 DSGVO): Prighter EU Rep GmbH, Schellinggasse 3/10, 1010 Wien

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber die Astrologie-Software Kosmogramm als Web-Anwendung (app.kosmogramm.com) bereit. Dabei verarbeitet er personenbezogene Daten, die der Auftraggeber in sein Konto eingibt, ausschließlich in dessen Auftrag.

(2) Der Vertrag gilt, solange das Kosmogramm-Konto des Auftraggebers besteht. Er endet automatisch mit dem Ende des Nutzungsvertrags; § 10 gilt darüber hinaus.

§ 2 Art, Zweck und Umfang der Verarbeitung

Zweck	Speichern der vom Auftraggeber angelegten Horoskope und Notizen; astrologische Berechnungen (Radix, Transite, Progressionen, Direktionen u. a.); Anzeige, Druck und Sicherung dieser Daten.
Art der Verarbeitung	Speichern, Berechnen, Anzeigen, tägliche Datensicherung, Löschen.
Arten von Daten	Name bzw. Bezeichnung, Geburtsdatum, Geburtszeit, Geburtsort mit Koordinaten und Zeitzone; Notizen, Stichworte und eigene Deutungstexte; Geburtstagsliste.
Betroffene Personen	Klientinnen und Klienten des Auftraggebers sowie weitere Personen, deren Daten der Auftraggeber einträgt (z. B. Angehörige).
Besondere Kategorien (Art. 9 DSGVO)	Nicht vorgesehen. Trägt der Auftraggeber in Notizen dennoch z. B. Gesundheitsangaben ein, verarbeitet der Auftragnehmer sie mit denselben

	Schutzmaßnahmen; für die Rechtsgrundlage ist der Auftraggeber verantwortlich.
Ort der Verarbeitung	Rechenzentrum in Frankfurt am Main (Deutschland). Eine Verarbeitung außerhalb der EU bzw. des EWR findet nicht statt.

Nicht Gegenstand dieses Vertrags sind die Daten des Kundenkontos selbst (E-Mail-Adresse, Name, Passwort, Zahlungsdaten). Diese verarbeitet der Auftragnehmer als eigener Verantwortlicher; siehe Datenschutzerklärung unter kosmogramm.com/datenschutz.

§ 3 Weisungen

- (1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers. Die Weisungen ergeben sich aus diesem Vertrag und aus der Bedienung der Software durch den Auftraggeber (z. B. Anlegen, Ändern und Löschen von Horoskopen). Weitere Weisungen erteilt der Auftraggeber per E-Mail.
- (2) Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin.
- (3) Eine Verarbeitung zu eigenen Zwecken, etwa zur Auswertung, Werbung oder zum Training von KI-Systemen, findet nicht statt.

§ 4 Vertraulichkeit

Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind. Zugriff auf den Server hat ausschließlich der Vertreter des Auftragnehmers; ein Zugriff auf Inhalte erfolgt nur, soweit es für Betrieb, Fehlerbehebung oder eine Weisung des Auftraggebers nötig ist.

§ 5 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in **Anlage 1** beschriebenen Maßnahmen nach Art. 32 DSGVO. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.

§ 6 Unterauftragsverarbeiter

- (1) Der Auftraggeber stimmt dem Einsatz der in **Anlage 2** genannten Unterauftragsverarbeiter zu.
- (2) Über einen geplanten Wechsel oder neuen Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber mindestens 30 Tage vorher per E-Mail. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen; ist keine Einigung möglich, darf er den Nutzungsvertrag fristlos kündigen.
- (3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Schutzniveau, das diesem Vertrag entspricht.

§ 7 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch). Die meisten Anfragen kann der Auftraggeber selbst in der Software erledigen. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich weiter.

(2) Er unterstützt den Auftraggeber außerdem bei Datenschutz-Folgenabschätzungen und bei der Zusammenarbeit mit Aufsichtsbehörden, soweit dies die hier verarbeiteten Daten betrifft.

§ 8 Datenschutzverletzungen

Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, per E-Mail. Die Meldung enthält, soweit bekannt, Art und Umfang der Verletzung, die wahrscheinlichen Folgen und die ergriffenen Maßnahmen.

§ 9 Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die Informationen bereit, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind. Kontrollen vor Ort sind nach rechtzeitiger Anmeldung zu üblichen Geschäftszeiten möglich; in der Regel genügt eine schriftliche Auskunft.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Bis zum Vertragsende kann der Auftraggeber seine Daten jederzeit selbst in der Software einsehen, drucken und löschen.

(2) Nach Vertragsende löscht der Auftragnehmer die Daten des Auftraggebers innerhalb von 30 Tagen. In den täglichen Datensicherungen sind sie danach noch höchstens 30 weitere Tage enthalten und werden dann automatisch überschrieben. Auf Wunsch bestätigt der Auftragnehmer die Löschung schriftlich.

§ 11 Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland. Die Haftung richtet sich nach Art. 82 DSGVO.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag geht dieser Vertrag in Fragen des Datenschutzes vor.

(3) Änderungen bedürfen der Textform (E-Mail genügt). Ist eine Bestimmung unwirksam, bleibt der Rest wirksam.

Ort, Datum, Unterschrift Auftraggeber

Ort, Datum, Unterschrift Auftragnehmer
Sebastian Schenkyr für DEFI PIONEER LLC

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- Server in einem Rechenzentrum in Frankfurt am Main; physische Zutrittskontrolle durch den Rechenzentrumsbetreiber.
- Zugang zum Server nur per SSH mit kryptografischem Schlüssel, Anmeldung per Passwort abgeschaltet; Firewall lässt nur Web- und SSH-Verkehr zu.
- Anmeldung in Kosmogramm mit persönlichem Konto; Passwörter werden nur als script-Hash gespeichert, nie im Klartext.
- Schutz gegen Passwort-Raten: Sperre nach 5 Fehlversuchen innerhalb von 15 Minuten.
- Strikte Trennung der Konten: Jedes Konto sieht ausschließlich die eigenen Horoskope, Notizen und Texte.
- Sitzungs-Cookie nur über HTTPS, nicht per Skript auslesbar (HttpOnly, SameSite); auf dem Server wird nur ein Hashwert davon gespeichert.

Integrität

- Alle Verbindungen verschlüsselt (TLS/HTTPS mit Zertifikat von Let's Encrypt); Sicherheits-Header gegen Einbettung und Skript-Einschleusung.
- Schreibende Anfragen werden nur von der eigenen Seite angenommen (Herkunftsprüfung).
- Änderungen an der Software werden vor der Freigabe automatisiert geprüft.

Verfügbarkeit und Belastbarkeit

- Tägliche automatische Datensicherung auf dem Server, Aufbewahrung 30 Tage.
- Automatischer Neustart des Dienstes bei Störungen; regelmäßige Sicherheitsupdates des Betriebssystems.

Überprüfung

- Server-Protokolle werden nach spätestens 14 Tagen gelöscht.
- Die Maßnahmen werden mindestens jährlich und nach jeder größeren Änderung überprüft.

Anlage 2 – Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hostinger International Ltd., 61 Lordou Vironos Street, 6023 Larnaca, Zypern	Bereitstellung des Servers (Hosting); Vertrag zur Auftragsverarbeitung als Anhang zu den Nutzungsbedingungen	Frankfurt am Main, Deutschland

Für Einladungs- und Passwort-E-Mails an den Auftraggeber nutzt der Auftragnehmer Brevo (Sendinblue SAS, Paris). Dabei werden nur Daten des Kundenkontos verarbeitet, keine Daten aus § 2; Brevo ist daher kein Unterauftragsverarbeiter im Sinne dieses Vertrags.