KI-NAVIGATOR
KI-Automation für KMU in Österreich

Auftragsverarbeitungs-vertrag (AVV)

Mustertext nach Art. 28 DSGVO

v1.0 · 12.06.2026

Dieser Mustertext bildet die Standard-Vorlage für den Auftragsverarbeitungsvertrag, der bei jedem KI-Navigator-Projekt mit Verarbeitung personenbezogener Daten geschlossen wird. Er deckt die Pflichtinhalte des Art. 28 DSGVO ab und beschreibt die konkret eingesetzten technisch-organisatorischen Maßnahmen sowie die Unterauftragsverarbeiter.

! WICHTIG - MUSTERVERTRAG, KEINE RECHTSBERATUNG

Dieser Mustertext dient als Diskussionsgrundlage und wird pro Projekt an die tatsächlich umgesetzten Verarbeitungen, Subprozessoren und technischen Maßnahmen angepasst. Er ersetzt keine individuelle Rechtsberatung. Vor Unterzeichnung empfehlen wir die Prüfung durch einen DSGVO-spezialisierten Rechtsanwalt. Verbindlich ist ausschließlich der finale, beidseitig unterzeichnete Vertrag.

Vertragsparteien (werden pro Projekt eingetragen)

VERANTWORTLICHER (Kunde)

[Firma]
[Adresse, PLZ Ort]
UID: ATU[...]
vertreten durch [Geschäftsführung]

AUFTRAGSVERARBEITER

KI-Navigator - Dieter Deutsch
Am Fluss 20, 8330 Feldbach
office@kinavigator.at
vertreten durch Dieter Deutsch

§ 1

Gegenstand, Dauer und Zweck der Verarbeitung

(1) Gegenstand:
Der Auftragsverarbeiter stellt dem Verantwortlichen einen KI-gestützten Workflow bereit (z.B. Email-Triage, KI-Mitarbeiter, Chatbot, Datenextraktion), der eingehende Kommunikation des Verantwortlichen klassifiziert, strukturiert oder Antwort-Entwürfe generiert. Der konkrete Funktionsumfang ergibt sich aus dem Hauptvertrag (Anbot / Auftragsbestätigung).

(2) Zweck:
Effizienzsteigerung der vom Verantwortlichen vorgegebenen Geschäftsprozesse. Die finale Entscheidung über jede aus dem Workflow resultierende Handlung (Versand, Vertragsabschluss, Bewertung) liegt ausschließlich beim Verantwortlichen oder seinen Mitarbeitern. Der Auftragsverarbeiter trifft keine automatisierten Einzelentscheidungen im Sinne des Art. 22 DSGVO.

(3) Art der Verarbeitung:
Erheben, Speichern, Strukturieren, Analysieren (Klassifikation), Pseudonymisieren (Ersetzen personenbezogener Bezeichner durch Tokens vor Übermittlung an Drittland-LLMs), Generieren (Antwort-Entwürfe), Re-Identifizieren (Rueck-Mapping innerhalb der EU), Löschen.

(4) Dauer:
Der Vertrag beginnt am Tag der Unterzeichnung durch beide Parteien und laeuft auf unbestimmte Zeit. Er kann von beiden Parteien mit einer Frist von drei (3) Monaten zum Monatsende ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberuehrt.

(5) Ort der Verarbeitung:
Europaeische Union (Hostinger-Server in der EU, Mistral AI in Frankreich). Eine Übermittlung an Anthropic (USA) erfolgt nur dann, wenn dies für den jeweiligen Workflow erforderlich ist und ausschließlich auf Grundlage von EU-Standardvertragsklauseln (siehe Anlage 2). Personenbezogene Bezeichner werden vor Übermittlung pseudonymisiert.

§ 2

Art der personenbezogenen Daten und Kategorien Betroffener

(1) Datenkategorien

- Identifikationsdaten (Vor- und Nachname, Email-Adresse)
- Kontaktdaten (Telefon, postalische Adresse, soweit in Inhalten enthalten)
- Vertrags- und Stammdaten (gemäß konkretem Hauptvertrag)
- Kommunikationsdaten (Betreff, Inhalt, Anhaenge, Zeitstempel)
- ggf. besondere Kategorien iSd Art. 9 DSGVO, wenn vom Betroffenen freiwillig in der Kommunikation mitgeteilt. Es ist nicht Zweck der Verarbeitung, solche Daten systematisch zu erheben.

(2) Kategorien betroffener Personen

- Kunden, Mieter, Eigentuemer, Mandanten, Interessenten des Verantwortlichen
- Lieferanten, Dienstleister, Geschäftspartner des Verantwortlichen
- Mitarbeiter und Vertreter des Verantwortlichen (als Absender / Empfaenger)
- Behördenvertreter (als Absender)

(3) Datenminimierung:
Der Verantwortliche stellt sicher, dass die an den Auftragsverarbeiter übermittelten Stamm- und Inhaltsdaten auf das für die jeweilige Verarbeitungstaetigkeit erforderliche Maß beschraenkt sind. Bank-, Geburts- oder Gesundheitsdaten werden ohne separate Vereinbarung nicht systematisch verarbeitet.

§ 3

Weisungen, Pflichten und Rechte

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich Übermittlungen in Drittländer. Die im Hauptvertrag und in diesem AVV beschriebenen Verarbeitungen gelten als dokumentierte Weisung iSd Art. 28 Abs. 3 lit. a DSGVO.

(2) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, hat er den Verantwortlichen unverzüglich zu informieren.

(3) Der Verantwortliche ist verantwortlich für die Rechtmäßigkeit der Datenverarbeitung gegenüber den Betroffenen, insbesondere für das Vorliegen einer Rechtsgrundlage iSd Art. 6 DSGVO und ggf. Art. 9 DSGVO.

§ 4

Vertraulichkeit

(1) Der Auftragsverarbeiter verpflichtet alle mit der Verarbeitung befassten Personen schriftlich zur Vertraulichkeit, sofern sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Diese Verpflichtung besteht auch nach Beendigung des Vertrags fort.

§ 5

Technische und organisatorische Maßnahmen (TOMs)

(1) Der Auftragsverarbeiter trifft die erforderlichen TOMs nach Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die konkreten Maßnahmen sind in Anlage 1 beschrieben.

(2) Wesentliche Änderungen der TOMs sind dem Verantwortlichen unverzüglich mitzuteilen. Der allgemeine Sicherheitsstandard darf dabei nicht abgesenkt werden.

§ 6

Unterauftragsverarbeiter (Subprozessoren)

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine schriftliche Genehmigung zur Beauftragung weiterer Auftragsverarbeiter gemäß Art. 28 Abs. 2 DSGVO. Die zum Zeitpunkt des Vertragsabschlusses eingesetzten Subprozessoren sind in Anlage 2 aufgeführt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens dreissig (30) Tage vor jeder beabsichtigten Hinzunahme oder Abloesung eines Subprozessors per Email an die in Anlage 3 genannte Kontaktadresse.

(3) Der Verantwortliche kann innerhalb von vierzehn (14) Tagen nach Erhalt der Mitteilung aus wichtigem datenschutzrechtlichem Grund Widerspruch einlegen. Erfolgt kein Widerspruch, gilt die Genehmigung als erteilt.

(4) Bei berechtigtem Widerspruch sind beide Parteien berechtigt, den Vertrag mit einer Frist von dreissig (30) Tagen zu kuendigen.

(5) Der Auftragsverarbeiter verpflichtet die Subprozessoren auf mindestens dieselben Datenschutzpflichten und bleibt gegenüber dem Verantwortlichen für die Einhaltung verantwortlich.

§ 7

Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit geeigneten Maßnahmen bei der Erfuellung der Pflichten aus Art. 12-22 DSGVO (Betroffenenrechte), insbesondere:

- Auskunftsrecht (Art. 15)
- Recht auf Berichtigung (Art. 16)
- Recht auf Löschung (Art. 17)
- Recht auf Einschraenkung (Art. 18)
- Recht auf Datenübertragbarkeit (Art. 20)
- Widerspruchsrecht (Art. 21)

(2) Wendet sich ein Betroffener direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich, spätestens innerhalb von drei (3) Werktagen, an den Verantwortlichen weiter und beantwortet sie nicht selbst.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen ferner bei den Pflichten gemäß Art. 32-36 DSGVO (Sicherheit, Meldung von Datenpannen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

§ 8

Meldung von Datenschutzverletzungen

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekanntwerdende Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von vierundzwanzig (24) Stunden nach Kenntniserlangung per Email an die in Anlage 3 genannte Kontaktadresse.

(2) Die Meldung enthaelt mindestens:

- Beschreibung der Art der Datenschutzverletzung
- Kategorien und ungefaehre Zahl der Betroffenen und Datensaetze
- Wahrscheinliche Folgen
- Ergriffene oder vorgeschlagene Gegenmassnahmen
- Kontaktstelle des Auftragsverarbeiters für Rueckfragen

§ 9

Löschung und Rueckgabe der Daten

(1) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen oder gibt sie auf dessen Wahl zurueck, sofern keine gesetzliche Aufbewahrungspflicht besteht.

(2) Die Löschung erfolgt innerhalb von dreissig (30) Tagen nach Vertragsende und umfasst Workflow-Daten, Logs, Caches und Backups in den vom Auftragsverarbeiter kontrollierten Systemen.

(3) Die Löschung ist dem Verantwortlichen schriftlich (per Email) zu bestaetigen.

§ 10

Kontroll- und Auditrechte

(1) Der Verantwortliche hat das Recht, sich von der Einhaltung dieses Vertrags und der TOMs zu überzeugen. Er kann hierfür:

- Schriftliche Auskuenfte und Selbstauskuenfte einfordern (z.B. SOC-2-Reports, ISO-27001-Zertifikate der Subprozessoren, soweit verfuegbar).
- Mit vorheriger Ankuendigung von mindestens vierzehn (14) Tagen waehrend üblicher Geschäftszeiten Inspektionen vor Ort durchführen oder durch beauftragte Dritte durchführen lassen.

(2) Mehr als eine Vor-Ort-Kontrolle pro Kalenderjahr ist nur bei konkretem Anlass (z.B. Datenschutzverletzung) ohne Kostenersatz zulässig; darüber hinausgehende Kontrollen können vom Auftragsverarbeiter zu seinen üblichen Stundensätzen berechnet werden.

§ 11

Haftung

Es gelten die gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO. Die Haftungsregelung des Hauptvertrags zwischen den Parteien bleibt im Uebrigen unberuehrt, soweit zwingende gesetzliche Bestimmungen nicht entgegenstehen.

§ 12

Schlussbestimmungen

(1) Änderungen und Ergaenzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit des uebrigen Vertrags unberuehrt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.

(3) Es gilt oesterreichisches Recht unter Ausschluss des UN-Kaufrechts. Gerichtsstand ist - soweit gesetzlich zulässig vereinbar - der Sitz des Auftragsverarbeiters (Feldbach, Steiermark).

(4) Dieser Vertrag tritt mit Unterzeichnung durch beide Parteien in Kraft.

UNTERSCHRIFTEN

Unterzeichnung des Vertrags

Mit Unterzeichnung beider Parteien tritt dieser Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO in Kraft. Beide Parteien bestaetigen, die Anlagen 1 (Technische und organisatorische Maßnahmen), 2 (Subprozessoren) und 3 (Kontaktstellen) zur Kenntnis genommen und akzeptiert zu haben.

Ort und Datum der Unterzeichnung

[Ort], am [Datum]

FUER DEN VERANTWORTLICHEN

Unterschrift

[Name, Funktion]
[Firma des Verantwortlichen]

FUER DEN AUFTRAGSVERARBEITER

Unterschrift

Dieter Deutsch
Geschäftsführer, KI-Navigator

Hinweis

Dieser Mustervertrag dient als Diskussionsgrundlage und wird pro Projekt an die tatsächlich umgesetzten Workflows angepasst. Verbindlich ist erst der finale, beidseitig unterzeichnete Vertrag. Vor Unterzeichnung empfehlen wir die Prüfung durch einen DSGVO-spezialisierten Rechtsanwalt.

Anlage 1

Technische und organisatorische Maßnahmen (TOMs)

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Server in EU-Rechenzentren mit physischer Zugangskontrolle (Hostinger - ISO 27001 zertifiziert).
- Zugangskontrolle: Multi-Faktor-Authentifizierung für alle Admin-Zugaenge (n8n, Anthropic Console, Mistral Console, Supabase Studio). Keine geteilten Accounts.
- Zugriffskontrolle: Rollenbasierte Berechtigungen in n8n (Owner / Member). Anthropic und Mistral Workspaces pro Kunde getrennt.
- Trennungskontrolle: Pro Kunde eigene n8n-Instanz auf Hostinger, eigener Anthropic-Workspace, eigener Mistral-API-Key. Kein Daten-Sharing zwischen Kunden.
- Pseudonymisierung und Verschluesselung: TLS 1.2+ für alle Verbindungen (IMAP, SMTP, HTTPS). Vor jedem Aufruf an Drittland-LLMs werden personenbezogene Bezeichner (Namen, Email-Adressen, Telefonnummern, IBAN) durch deterministische Tokens ersetzt. Das Token-Original-Mapping verbleibt in der EU-n8n-Instanz und wird nicht an Drittländer übermittelt.

Integritaet (Art. 32 Abs. 1 lit. b DSGVO)

- Eingabekontrolle: n8n-Workflow-Execution-Logs mit Timestamp und Node-Status (30 Tage Retention).
- Weitergabekontrolle: Verschluesselte Übertragung über alle Strecken (TLS).

Verfuegbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfuegbarkeitskontrolle: Hostinger Cloud-Backup taeglich, 7 Tage Retention.
- Rasche Wiederherstellbarkeit: Workflow-Definitionen versioniert im KI-Navigator-Repository (Git).

Verfahren zur regelmäßigen Überpruefung (Art. 32 Abs. 1 lit. d DSGVO)

- Datenschutz-Management: Jaehrliche Überpruefung der TOMs.
- Vorfallsmanagement: Definierter Meldeweg gemäß § 8 dieses Vertrags.
- Auftragskontrolle: Subprozessoren-Liste jährlich überprueft (siehe Anlage 2).

Anlage 2

Liste der Subprozessoren

Stand 12.06.2026. Änderungen werden gemäß § 6 Abs. 2 angekündigt. Die nachfolgenden Subprozessoren werden eingesetzt, soweit für den im Hauptvertrag beschriebenen Workflow erforderlich.

1. Hostinger International Ltd.

Verarbeitung:

Hosting der dedizierten n8n-Instanz, temporaere Speicherung von Workflow-Daten waehrend Verarbeitung.

Ort:

Litauen (EU)

Rechtsgrundlage Drittland:

EU - keine zusaetzliche Rechtsgrundlage erforderlich.

2. Mistral AI SAS

Verarbeitung:

KI-Klassifikation und Strukturierung von Inhalten (z.B. Email-Kategorisierung, Information-Extraction).

Ort:

Frankreich (EU)

Rechtsgrundlage Drittland:

EU - keine zusaetzliche Rechtsgrundlage erforderlich.

3. Anthropic, PBC (nur bei Bedarf)

Verarbeitung:

Generierung von Antwort-Entwürfen oder komplexen Sprachverarbeitungs-Aufgaben (Claude-API). Aufruf ausschließlich mit pseudonymisiertem Text: personenbezogene Bezeichner (Namen, Email, Telefonnummern, IBAN) werden vor Übermittlung durch Tokens wie [PERSON_1] ersetzt. Das Mapping verbleibt in der EU.

Ort:

USA (mit EU-Inference-Option, wo verfuegbar)

Rechtsgrundlage Drittland:

EU-Standardvertragsklauseln (SCC, Modul 2), Anthropic DPA, Zero-Retention-API-Modus.

Hinweise

- Alle Subprozessoren erhalten ausschließlich die für ihre jeweilige Verarbeitungstaetigkeit notwendigen Daten.
- API-Aufrufe an Mistral und Anthropic erfolgen ohne persistente Logs auf Seite der Subprozessoren (siehe jeweilige DPAs).
- Sensitive Kategorien (Kündigung, Behörde, Beschwerde, Gesundheit) werden, sofern technisch im Workflow vorgesehen, automatisch von der LLM-Verarbeitung ausgeschlossen und direkt an einen menschlichen Sachbearbeiter weitergeleitet.

Anlage 3

Kontaktstellen

Auftragsverarbeiter (Datenschutz-Anfragen, Datenpannen-Meldungen)

- Verantwortliche Person: Dieter Deutsch (Geschäftsführung)
- Email: office@kinavigator.at
- Telefon: +43 664 1481403
- Anschrift: Am Fluss 20, 8330 Feldbach, Steiermark, Österreich

Verantwortlicher (wird pro Projekt eingetragen)

- Verantwortliche Person: [Name, Funktion]
- Email: [datenschutz@kunde.at]
- Telefon: [+43 ...]
- Anschrift: [Strasse, PLZ Ort, Land]

Hinweis zur Verwendung

Dieser Mustertext ist Ausgangspunkt der Vertragsverhandlung. Der finale, beidseitig unterzeichnete AVV wird pro Projekt an die tatsächlich umgesetzten Workflows, Subprozessoren und Sicherheitsmassnahmen angepasst. Wir empfehlen die Prüfung durch einen DSGVO-spezialisierten Rechtsanwalt vor Unterzeichnung.