Vereinbarung zur Auftragsbearbeitung (AVV) – Anhang 1 zu den AGB, Anlage zu den Cloud-Pilot-Bedingungen

Fassung 1.1 vom 11. November 2026 (ersetzt 1.0 vom 28. Oktober 2026).

ENTWURF 1.1 · 11. November 2026 · nicht anwaltlich geprüft, keine Rechtsberatung, ohne Gewähr – Prüfung durch Fachperson Recht offen.

1 Gegenstand und Rollen

1.1 Diese Vereinbarung regelt die Bearbeitung von Personendaten durch die Firnkern GmbH in Gründung, Bosenhaldenweg 26, 4125 Riehen, Schweiz, vertreten durch Marco Grieshaber, Gründer und Geschäftsführer («Firnkern», «Auftragsbearbeiterin»), im Auftrag des Kunden bzw. Pilotbetriebs («Kunde», «Verantwortlicher») bei:

a) dem Betrieb einer Instanz der Software Firnkern Server durch Firnkern – im Pilot als «Firnkern-Cloud (Pilot)» nach den Cloud-Pilot-Bedingungen 1.0, nach dem Verkaufsstart als Cloud-Betrieb nach AGB Teil C;

b) «KI über Firnkern» (Vermittlungsdienst ki.firnkern.com), im Pilot nach dem Zusatz «KI über Firnkern im Pilot» 1.0;

c) Support mit Einsicht in Inhalte, wenn der Kunde dies im Einzelfall verlangt.

1.2 Sie erfüllt Art. 9 DSG und, soweit anwendbar, Art. 28 DSGVO. Die Begriffe des DSG («Personendaten», «bearbeiten», «Auftragsbearbeiter») entsprechen den Begriffen der DSGVO («personenbezogene Daten», «verarbeiten», «Auftragsverarbeiter»).

1.3 Beim Betrieb im Firmennetz des Kunden mit eigenem KI-Konto bearbeitet Firnkern keine Inhalte des Kunden; diese Vereinbarung gilt dann nicht. Für Angaben, die Firnkern als eigene Verantwortliche bearbeitet (Einrichtung der Instanz, Zustimmungsprotokoll, Rückmeldungen über den Meldedienst, Lizenz und Aktivierung, Abrechnung), gilt die Datenschutzerklärung von Firnkern.

2 Art, Zweck und Dauer der Bearbeitung

Punkt	Inhalt
Zweck	Cloud: Betrieb einer eigenen Instanz der Software für den Kunden (speichern, anzeigen, übertragen, sichern, wiederherstellen, exportieren, löschen). KI über Firnkern: Weiterleitung von Ton zur Mitschrift und pseudonymisierten Textauszügen an Sprachmodelle. Support: Einsicht im Einzelfall auf Wunsch.
Art der Bearbeitung	Hosting, Speicherung, Sicherung, Wiederherstellung, Export, Löschung; Durchleitung an KI-Anbieter ohne Speicherung von Inhalten
Datenkategorien und betroffene Personen	siehe Anhang 3
Besonders schützenswerte Personendaten	nicht vorgesehen; der Kunde vermeidet sie in Inhalten. Erfasst er sie trotzdem, ist er dafür verantwortlich.
Ort	Schweiz (Anhang 2). Eine Bekanntgabe in die USA erfolgt nur, wenn der Admin «KI über Firnkern» Stufe 3 einschaltet.
Dauer	Laufzeit des Cloud-Pilots bzw. Cloud-Vertrags und von «KI über Firnkern», zuzüglich der Fristen nach Ziffer 8

3 Weisungen

3.1 Firnkern bearbeitet Personendaten nur auf dokumentierte Weisung des Kunden. Weisungen sind diese Vereinbarung, die Cloud-Pilot-Bedingungen bzw. der Vertrag, die Einstellungen, die der Admin in der Software wählt (zum Beispiel KI-Stufen, Meldedienst), sowie Weisungen in Textform (E-Mail an marco@firnkern.com) von dazu berechtigten Personen des Kunden. Das gilt auch für eine Bekanntgabe ins Ausland: Stufe 3 (USA) wird nur genutzt, wenn der Admin sie einschaltet.

3.2 Ist Firnkern gesetzlich zu einer anderen Bearbeitung verpflichtet, teilt Firnkern dies dem Kunden vorher mit, sofern das Gesetz eine solche Mitteilung nicht verbietet.

3.3 Hält Firnkern eine Weisung für rechtswidrig, teilt Firnkern dies dem Kunden unverzüglich mit und kann die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.

3.4 Firnkern nutzt die Daten nicht für eigene Zwecke, insbesondere nicht zum Training von KI-Modellen, und gibt sie nur nach dieser Vereinbarung weiter.

4 Vertraulichkeit

4.1 Personen, die bei Firnkern Zugang zu Daten haben könnten, sind schriftlich zur Vertraulichkeit verpflichtet, auch über das Ende ihrer Tätigkeit hinaus.

4.2 Firnkern sieht keine Inhalte ein, ausser der Kunde verlangt es im Einzelfall (zum Beispiel für Support) oder es ist für Export, Wiederherstellung, Löschung oder die Abwehr einer akuten Sicherheitsgefahr unumgänglich. Firnkern informiert den Kunden in diesem Fall.

5 Datensicherheit

5.1 Firnkern trifft die technischen und organisatorischen Massnahmen nach Anhang 1 (Art. 8 DSG, Art. 32 DSGVO) und hält sie auf einem dem Risiko angemessenen Stand. Firnkern darf sie ändern, wenn das Schutzniveau nicht sinkt; wesentliche Änderungen teilt Firnkern dem Kunden mit.

5.2 Anhang 1 nennt offen, was noch nicht umgesetzt ist, insbesondere den zweiten Standort für die Sicherungen.

6 Unterauftragsbearbeiter

6.1 Der Kunde genehmigt die Unterauftragsbearbeiter in Anhang 2 (allgemeine Genehmigung). Unterauftragsbearbeiter für KI werden nur tätig, wenn der Admin die entsprechende Funktion einschaltet.

6.2 Firnkern informiert den Kunden mindestens 30 Tage vor dem Beizug oder Wechsel eines Unterauftragsbearbeiters per E-Mail. Der Kunde kann innert dieser Frist aus wichtigem Grund widersprechen; im Pilot kann er den Cloud-Pilot dann mit sofortiger Wirkung beenden (Export und Löschung nach Ziffer 8), sonst den betroffenen Vertrag auf den Zeitpunkt der Änderung kündigen.

6.3 Firnkern verpflichtet Unterauftragsbearbeiter vertraglich auf gleichwertige Datenschutzpflichten und bleibt dem Kunden gegenüber für deren Erfüllung verantwortlich.

6.4 Eine Bekanntgabe ins Ausland erfolgt nur in Staaten mit angemessenem Datenschutz oder mit geeigneten Garantien (Art. 16 DSG; Art. 46 DSGVO), zum Beispiel Standardvertragsklauseln. Im Cloud-Pilot liegen die Inhalte in der Schweiz.

7 Unterstützung des Kunden

7.1 Betroffenenrechte: Firnkern unterstützt den Kunden mit den Funktionen der Software (Export, Berichtigen, Löschen) und auf Anfrage bei Begehren betroffener Personen. Wendet sich eine betroffene Person direkt an Firnkern, leitet Firnkern das Begehren unverzüglich an den Kunden weiter und beantwortet es nur auf seine Weisung.

7.2 Verletzung der Datensicherheit: Firnkern meldet dem Kunden eine Verletzung, die seine Daten betrifft, unverzüglich, spätestens innert 48 Stunden nach Kenntnis (vgl. Art. 24 Abs. 3 DSG; Art. 33 Abs. 2 DSGVO), per E-Mail an den Admin bzw. die Ansprechperson. Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien und ungefähre Zahl der Betroffenen, wahrscheinliche Folgen, getroffene oder vorgeschlagene Massnahmen, Kontaktstelle. Fehlende Angaben liefert Firnkern laufend nach.

7.3 Hinweis: Der Kunde als Verantwortlicher meldet eine Verletzung, die voraussichtlich zu einem hohen Risiko führt, dem EDÖB so rasch als möglich (Art. 24 Abs. 1 DSG); soweit die DSGVO gilt, meldet er sie der Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden (Art. 33 Abs. 1 DSGVO). Die Frist nach Ziffer 7.2 soll ihm das ermöglichen.

7.4 Datenschutz-Folgenabschätzung: Firnkern stellt dem Kunden die nötigen Angaben zur Verfügung (diese Vereinbarung mit Anhängen, Beschreibung der Software, Merkblatt Betriebsrat und Personalvertretung) und unterstützt ihn auf Anfrage bei einer Folgenabschätzung oder Konsultation der Behörde (Art. 22 DSG; Art. 35, 36 DSGVO).

7.5 Im Pilot ist die Unterstützung unentgeltlich. Nach dem Verkaufsstart vereinbaren die Parteien den Aufwand, der über die Funktionen der Software hinausgeht gesondert.

8 Rückgabe und Löschung

8.1 Der Kunde kann seine Daten jederzeit exportieren.

8.2 Cloud-Pilot: Am Ende erhält der Kunde einen Schluss-Export. Danach löscht Firnkern die Instanz, das Datenvolume und alle Sicherungen (auch am zweiten Standort, sobald eingerichtet), spätestens 30 Tage nach dem Ende, früher, sobald der Kunde den Empfang des Schluss-Exports bestätigt. Firnkern protokolliert die Löschung und bestätigt sie auf Wunsch per E-Mail.

8.3 Cloud-Betrieb nach dem Verkaufsstart: Nach Vertragsende kann der Kunde seine Daten 30 Tage lang exportieren; danach löscht Firnkern die Daten einschliesslich Sicherungen innert weiterer 30 Tage (AGB Ziffer C3).

8.4 «KI über Firnkern»: Der Vermittlungsdienst speichert keine Inhalte. Gespeichert werden nur Zeit, Kunde, Dienst, Menge, Kosten und Status, zur Vermeidung doppelter Verrechnung während 24 Stunden eine Prüfsumme einer Tondatei, nie der Ton selbst. Diese Verbrauchsdaten löscht Firnkern 12 Monate nach dem Ende des Pilots bzw. des Guthabens.

8.5 Besteht eine gesetzliche Aufbewahrungspflicht, sperrt Firnkern die betroffenen Daten und nutzt sie nur dafür.

9 Nachweise und Kontrolle

9.1 Firnkern stellt dem Kunden die nötigen Informationen zum Nachweis dieser Pflichten zur Verfügung, insbesondere diese Vereinbarung mit Anhängen, den Auszug aus dem Verzeichnis der Bearbeitungstätigkeiten und Auszüge aus den Protokollen (Sicherung, Überwachung, Löschung) ohne Daten anderer Kunden.

9.2 Prüfungen durch den Kunden oder eine von ihm beauftragte, zur Verschwiegenheit verpflichtete Person sind nach Vereinbarung möglich, höchstens einmal pro Jahr, mit 30 Tagen Vorlauf und auf Kosten des Kunden, ausser bei einem begründeten Verdacht auf eine Verletzung. Für die Rechenzentren der Unterauftragsbearbeiter gelten deren Nachweise. Daten anderer Kunden bleiben geschützt.

10 Haftung

Im Pilot gelten für die Haftung die Pilotvereinbarung (Ziffer 8) und die Cloud-Pilot-Bedingungen, sonst die AGB von Firnkern. Zwingende Bestimmungen des Datenschutzrechts bleiben vorbehalten.

11 Abschluss, Dauer und Schlussbestimmungen

11.1 Abschluss: Der Kunde nimmt diese Vereinbarung an, indem der Admin in der Software zustimmt – bei der Einrichtung der Instanz bzw. vor dem Einschalten von «KI über Firnkern» – mit den Häkchen «Ich habe die Bedingungen und die Auftragsbearbeitung gelesen und stimme zu» und «Ich bin berechtigt, für den Betrieb zuzustimmen». Firnkern speichert Fassung, Name, Login und Zeitpunkt in einem Protokoll und stellt dem Kunden auf Wunsch einen Auszug zu. Firnkern nimmt durch die Bereitstellung der Instanz bzw. des Dienstes an. Auf Wunsch unterzeichnen die Parteien zusätzlich.

11.2 Form: Soweit die DSGVO gilt, ist diese Vereinbarung schriftlich abzufassen, was auch in elektronischer Form erfolgen kann (Art. 28 Abs. 9 DSGVO). Die Zustimmung in der Software mit Protokoll soll diese Form erfüllen.

11.3 Dauer: Diese Vereinbarung gilt, solange Firnkern Personendaten im Auftrag des Kunden bearbeitet. Ziffern 4, 8 und 9 gelten über das Ende hinaus.

11.4 Vorrang: In Datenschutzfragen geht diese Vereinbarung den AGB, der Pilotvereinbarung und den Cloud-Pilot-Bedingungen vor. Der Zusatz «KI über Firnkern im Pilot» 1.0 präzisiert sie.

11.5 Gesellschaft in Gründung: Bis zum Eintrag im Handelsregister handelt Marco Grieshaber für die Gesellschaft; nach dem Eintrag tritt die Firnkern GmbH in diese Vereinbarung ein.

11.6 Es gilt schweizerisches Recht; Gerichtsstand gemäss Pilotvereinbarung bzw. AGB. Soweit die DSGVO anwendbar ist, bleiben ihre zwingenden Bestimmungen vorbehalten. Massgebend ist die deutsche Fassung.

Bereich	Massnahme	Stand
Rechenzentrum	Server Infomaniak VPS Cloud (Infomaniak Network SA, Genf), Rechenzentrum in der Schweiz; physische Sicherheit durch Infomaniak	in Betrieb (Angabe Infomaniak)
Trennung	je Betrieb eigener Container, eigenes Datenvolume, eigenes Netz; Instanzen erreichen sich nicht	in Betrieb
Übertragung	TLS mit Zertifikaten von Let's Encrypt (über Caddy); Adresse je Betrieb https://<name>.app.firnkern.com	in Betrieb
Anmeldung	Passwort und Pflicht-Zwei-Faktor (TOTP) oder Passkey (WebAuthn); Rechte nach Rolle in der Software; Passwörter und Sitzungen nur als Hash	in Betrieb
Admin-Zugang Firnkern	nur per SSH-Schlüssel; nur von der Geschäftsführung bestimmte, zur Vertraulichkeit verpflichtete Personen	in Betrieb
Netz	Firewall; offen nur die Ports 22 (SSH), 80 (Weiterleitung, Zertifikat) und 443 (HTTPS)	in Betrieb
Updates	automatische Sicherheitsupdates des Betriebssystems; Updates der Software durch Firnkern	in Betrieb
Überwachung	Prüfung alle 10 Minuten	in Betrieb
Sicherung	täglich 02:30 Uhr, verschlüsselt mit age (öffentlicher Schlüssel auf dem Server, privater Schlüssel nur offline bei Firnkern), 30 Tage aufbewahrt	in Betrieb

Bereich	Massnahme	Stand
Zweitstandort	Infomaniak Swiss Backup (Schweiz)	IN ARBEIT – bis dahin liegen die Sicherungen auf demselben Server
Wiederherstellung	Test der Wiederherstellung aus der Sicherung: mindestens vierteljährlich, erster Test vor Aufnahme echter Pilotdaten	offen
Ruhende Daten	Sicherungen verschlüsselt; Verschlüsselung des Datenvolumes: nicht zusätzlich verschlüsselt (Schutz durch Zugriffsbeschränkung des Servers)	teilweise
Protokolle	Betriebsprotokoll von Firnkern (betrieb.log) ohne Personendaten; Protokolle in der Instanz (zum Beispiel Anmeldungen) gehören zu den Inhalten des Kunden	in Betrieb
Verfügbarkeit	keine Zusage im Pilot; Infomaniak sagt Firnkern 99,99 % zu (gilt nur zwischen Infomaniak und Firnkern)	–
KI über Firnkern	nur nach Einschalten durch den Admin; Pseudonymisierung von Text vor Stufe 2 und 3, soweit die Software dies vorsieht; Ton nur mit Einwilligung; keine Speicherung von Inhalten im Vermittlungsdienst; Protokoll der Sendungen auf der Seite «KI und Datenschutz»	in Betrieb (Pilot)
Export und Löschung	Export jederzeit; Schluss-Export; Löschung von Instanz, Volume und Sicherungen mit Löschprotokoll (geloescht.log)	gebaut
Organisation	Meldeablauf für Sicherheitsvorfälle (Bewertung innert 4 Stunden, Meldung an Kunden nach Ziffer 7.2); interne KI-Richtlinie: keine Inhalte aus Instanzen in Entwicklungs- oder KI-Werkzeuge von Firnkern	Entwurf in Kraft

Anbieter	Leistung	Ort	Grundlage	Wann tätig
Infomaniak Network SA, Genf	Server der Firnkern-Cloud (VPS Cloud), Datenvolume, Sicherung auf dem Server	Schweiz («in der Schweiz gehostet», Angabe Infomaniak)	Schweizer Recht; Auftragsbearbeitungsvertrag von Infomaniak (abgelegt 10.11.2026)	immer im Cloud-Pilot
Infomaniak Network SA, Genf	Swiss Backup – zweiter Standort der Sicherungen	Schweiz	wie oben	sobald eingerichtet (Mitteilung nach Ziffer 6.2)
Infomaniak Network SA, Genf	Server des Vermittlungsdienstes ki.firnkern.com	Schweiz (Infomaniak, Rechenzentrum in der Schweiz)	wie oben	nur bei «KI über Firnkern»
Infomaniak Network SA, Genf	Sprachmodell (Modell Mistral) und Mitschrift, Stufe 2	Schweiz (laut Infomaniak durchgehend in der Schweiz)	wie oben	nur wenn der Admin «KI über Firnkern» einschaltet
Anthropic, PBC, San Francisco	Sprachmodell, Stufe 3; pseudonymisierte Textauszüge	USA	Standardvertragsklauseln im Data Processing Addendum von Anthropic (gültig ab 24.02.2025, mit Swiss Addendum; abgelegt 10.11.2026)	nur wenn der Admin Stufe 3 einschaltet (im Lieferzustand aus)

Kategorie	Beispiele	Betroffene Personen
Angaben zu Nutzenden	Name, Login, E-Mail (optional), Rolle, Rechte; Anmeldemerkmale (Passwort nur als Hash, Daten für Zwei-Faktor und Passkey)	Mitarbeitende, Kader und Leitung, Lernende, Studierende, Mentorinnen und Mentoren, weitere vom Kunden berechtigte Personen
Wissensinhalte	Wissen und Dossiers zu Rollen, Aufgabenblätter, Fragen und Antworten, Unterlagen, Mitschriften	Wissensgebende, Nachfolge, Prüfende; in Inhalten genannte Dritte (zum Beispiel Kontakte von Kunden oder Lieferanten)
Ton und Bild	Tonaufnahmen, Fotos, Videos – nur mit Einwilligung der jeweiligen Person	aufgenommene Personen
Kommunikation	Nachrichten zwischen Mitarbeitenden in der Software	Absender und Empfänger

Bereich	Massnahme	Stand
Lernen und Einarbeitung	Lernstand, Stand der Einarbeitung, Freigaben und Prüfungen von Übergaben (keine Bewertung von Personen durch die Software)	Lernende, Nachfolge, Mentees
Protokolle in der Instanz	Anmeldungen, Änderungen, Freigaben, Sendungen an KI-Anbieter (Zeit, Login, gegebenenfalls IP-Adresse)	Nutzende
KI über Firnkern	Ton zur Mitschrift und pseudonymisierte Textauszüge (nur durchgeleitet); Verbrauchsdaten (Zeit, Kunde, Dienst, Menge, Kosten)	Nutzende und in Inhalten genannte Personen
Besonders schützenswerte Personendaten	nicht vorgesehen; nur, wenn der Kunde sie selbst erfasst (dann in seiner Verantwortung)	–

Anforderung	Fundstelle in dieser Vereinbarung
Art. 28 Abs. 3 Einleitung DSGVO: Gegenstand, Dauer, Art, Zweck, Datenarten, Kategorien Betroffener, Pflichten und Rechte des Verantwortlichen	Ziffern 1, 2, Anhang 3
lit. a: Bearbeitung nur auf dokumentierte Weisung, auch für Übermittlungen in Drittländer	Ziffer 3
lit. b: Vertraulichkeit der befugten Personen	Ziffer 4
lit. c: Massnahmen nach Art. 32 DSGVO	Ziffer 5, Anhang 1
lit. d: Bedingungen für weitere Auftragsverarbeiter	Ziffer 6, Anhang 2
lit. e: Unterstützung bei Betroffenenrechten	Ziffer 7.1
lit. f: Unterstützung bei Art. 32–36 DSGVO	Ziffern 5, 7.2–7.4
lit. g: Löschung oder Rückgabe nach Abschluss	Ziffer 8
lit. h: Nachweise und Überprüfungen	Ziffer 9
Art. 28 Abs. 9 DSGVO: schriftlich, auch elektronisch	Ziffer 11.1, 11.2
Art. 9 Abs. 1 DSG: Bearbeitung nur so, wie der Verantwortliche es selbst tun dürfte	Ziffer 3
Art. 9 Abs. 2 DSG: Verantwortlicher vergewissert sich der Datensicherheit	Ziffer 5, Anhang 1, Ziffer 9
Art. 9 Abs. 3 DSG: Übertragung an Dritte nur mit vorgängiger Genehmigung	Ziffer 6
Art. 24 Abs. 3 DSG: Meldung an den Verantwortlichen so rasch als möglich	Ziffer 7.2