Auftragsverarbeitungs-Vertrag (AVV) nach Art. 28 DSGVO

Keysers Services UG (haftungsbeschränkt) Geschäftsführer: Sven Keysers · Sitz: Falkensee Marke: Financial Integrity Partners (“FIP”)

Stand: 2026-05-28 · Version: 1.1 · AVV-Nr.: [NR] · Datum: [DATUM]

---

§ 1 Vertragsparteien und Gegenstand

(1) Dieser Auftragsverarbeitungs-Vertrag (“AVV”) nach Art. 28 DSGVO wird geschlossen zwischen:

- **FIP** als **Auftragsverarbeiter**: Keysers Services UG (haftungsbeschränkt), Sitz Falkensee, vertreten durch den Geschäftsführer Sven Keysers, handelnd unter der Marke „Financial Integrity Partners";
- **Mandant** als **Verantwortlicher**: [FIRMA], [SITZ], vertreten durch [NAME, FUNKTION].

(2) **Gegenstand der Verarbeitung:** FIP verarbeitet im Auftrag des Mandanten personenbezogene Daten zur Erbringung datenanalytischer Leistungen — insbesondere zur Identifikation von Recovery-, Preventive-, Compliance- und Process-Findings auf Basis vom Mandanten bereitgestellter Buchungs- und Stammdaten.

(3) **Dauer der Verarbeitung:** Gekoppelt an die Laufzeit des jeweiligen Engagements (kostenloser Potenzial-Check, Leistungsstufe 1 Diagnostik mit Lifecycle, Leistungsstufe 2 Erfolgshonorar oder Leistungsstufe 3 Mandat) gemäß AGB und Engagement Letter, einschließlich vereinbarter Survival- und Löschfristen.

(4) **Rangordnung:** Bei Widersprüchen zwischen diesem AVV, der NDA, den AGB und dem Engagement Letter gilt der AVV vorrangig für **alle datenschutzrechtlichen und auftragsverarbeitungsbezogenen Regelungen**. Zwingende gesetzliche Anforderungen — insbesondere DSGVO und BDSG — bleiben unberührt.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung umfasst folgende Verarbeitungs-Tätigkeiten:

(1) **Einlesen und Aufbereitung** der vom Mandanten bereitgestellten Daten (insbesondere AP- und/oder AR-Exporte aus ERP-Systemen);

(2) **Engine-Scan und Finding-Generierung** durch die FIP-Detection-Engine inkl. LLM-gestützter Auswertungen;

(3) **Portalbetrieb:** Bereitstellung der Findings im Mandanten-Portal mit interaktiver Bearbeitung, Workflow-Hub und Status-Updates;

(4) **Re-Scan und Delta-Analysen** (in Leistungsstufe 2 und Leistungsstufe 3) zur fortlaufenden Identifikation neuer Findings sowie zur EDR-Berechnung;

(5) **Support und Anfragenbearbeitung** im Zusammenhang mit Findings, Widersprüchen und Portal-Nutzung;

(6) **Anonymisierung** für Engine-Weiterentwicklung gemäß § 15;

(7) **Löschung oder Rückgabe** nach Beendigung des Mandats gemäß § 11.

§ 3 Kategorien personenbezogener Daten

Ausschluss besonderer Kategorien: Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO (insbesondere Gesundheits-, Religions-, ethnische, gewerkschaftliche oder biometrische Daten) ist im Standard-Setup ausgeschlossen, soweit nicht im Engagement Letter oder in einer gesonderten AVV-Anlage ausdrücklich vereinbart.

Die Verarbeitung umfasst folgende Kategorien:

(1) **Stammdaten** von Lieferanten und Kunden des Mandanten (Name, Anschrift, Ansprechpartner, Kontaktdaten, Steuer-/USt-IDs);

(2) **Buchungs-Metadaten** (Belegnummern, Beträge, Buchungs- und Belegdaten, Konten, Kostenstellen);

(3) **Kommunikations-Inhalte** (soweit in Belegen, Anhängen oder Lieferanten-Korrespondenz enthalten);

(4) **Bankdaten** (Kontonummern, IBAN, BIC), soweit in Belegen enthalten;

(5) **Mandanten-eigene Stammdaten** der mit FIP interagierenden Personen (Buchhaltung, AP/AR-Owner, Reviewer).

§ 4 Kategorien betroffener Personen

(1) Mitarbeiter, Geschäftsführer und Ansprechpartner von Lieferanten und Kunden des Mandanten;

(2) Eigene Mitarbeiter des Mandanten (insbesondere Buchhaltung, AP/AR-Owner, Compliance, Reviewer);

(3) Sonstige natürliche Personen, soweit ihre Daten in den übermittelten Belegen enthalten sind.

§ 5 Pflichten und Rechte des Verantwortlichen (Mandant)

(1) Der Mandant ist als Verantwortlicher für die **Rechtmäßigkeit der Verarbeitung** und für die Erfüllung der Informationspflichten gegenüber den betroffenen Personen (Art. 13/14 DSGVO) verantwortlich.

(2) Dem Mandanten steht nach Art. 28 Abs. 3 lit. a DSGVO ein auf den **datenschutzrechtlichen Verarbeitungsrahmen** beschränktes Weisungsrecht zu. Es umfasst insbesondere Weisungen zur Art, zum Umfang, zum Zweck und zur Dauer der Verarbeitung sowie zum Umgang mit Betroffenen-Anfragen, nicht jedoch dienstvertragliche oder werkvertragliche Weisungen zur Erbringung der analytischen Leistung. Weisungen werden in Textform erteilt; mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Mandant hat **Auskunfts- und Audit-Rechte** gemäß § 14.

(4) Der Mandant stellt sicher, dass die Übermittlung personenbezogener Daten an FIP **rechtmäßig** ist (Rechtsgrundlage nach Art. 6 DSGVO bzw. Art. 9 DSGVO bei besonderen Kategorien).

§ 6 Pflichten von FIP als Auftragsverarbeiter

FIP verpflichtet sich insbesondere zu:

(1) **Verarbeitung ausschließlich auf dokumentierte Weisung** des Mandanten, soweit nicht durch Unionsrecht oder mitgliedstaatliches Recht etwas anderes vorgeschrieben ist. Als dokumentierte Hauptweisung gelten dieser AVV einschließlich seiner Anlagen sowie der zugehörige Engagement Letter; zusätzliche Einzelweisungen erfolgen in Textform (E-Mail oder Portal-Nachricht);

(2) Sicherstellung, dass die zur Verarbeitung befugten Personen sich zur **Vertraulichkeit** verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

(3) Einhaltung der **technisch-organisatorischen Maßnahmen** gemäß § 7 und TOMs-Anlage;

(4) **Unterstützung des Mandanten** bei der Beantwortung von Anfragen betroffener Personen (siehe § 12) und bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO;

(5) **Meldung von Datenschutzvorfällen** innerhalb von 24 Stunden nach Kenntnisnahme (siehe § 13);

(6) **Datenschutz-Folgenabschätzung-Unterstützung** gemäß Art. 35 DSGVO, soweit erforderlich;

(7) **Löschung oder Rückgabe** sämtlicher personenbezogener Daten nach Beendigung der Verarbeitung gemäß § 11;

(8) Bereitstellung aller erforderlichen **Nachweise zur Einhaltung der Pflichten** aus Art. 28 DSGVO.

§ 7 Technisch-organisatorische Maßnahmen (TOMs)

(1) FIP unterhält geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die konkreten Maßnahmen sind in der **TOMs-Anlage Stufe 1** beschrieben (Standard-Setup; Stufe 2 und Stufe 3 siehe § 9).

(2) FIP überprüft die TOMs regelmäßig (mindestens jährlich) und passt sie bei Bedarf an den Stand der Technik an. Wesentliche Änderungen werden dem Mandanten in Textform angezeigt.

(3) Die jeweils gültige TOMs-Anlage ist Bestandteil dieses AVV.

§ 8 Sub-Auftragsverarbeiter

(1) Der Mandant erteilt FIP die **allgemeine Genehmigung** zur Beauftragung der in der **Sub-Auftragsverarbeiter-Liste (Anlage 2)** genannten Sub-Auftragsverarbeiter. Anlage 2 ist Bestandteil dieses AVV und wird versioniert geführt; die jeweils aktuelle Fassung kann der Mandant beim Unternehmen anfordern.

(2) **Allgemeine Genehmigung mit Widerspruchsrecht:** Will FIP weitere Sub-Auftragsverarbeiter beauftragen oder bestehende ersetzen, teilt FIP dem Mandanten dies mit einer Vorlaufzeit von **30 Kalendertagen** in Textform mit. Innerhalb dieser Frist kann der Mandant der Hinzuziehung in Textform widersprechen. Im Widerspruchsfall ist der Mandant berechtigt, den Vertrag aus wichtigem Grund außerordentlich zu kündigen.

(3) FIP stellt sicher, dass die Sub-Auftragsverarbeiter **gleichwertige Datenschutzpflichten** wie in diesem AVV vereinbart sind, einschließlich Verpflichtungen zu TOMs und Vertraulichkeit.

§ 9 Erweiterte Datenschutz-Stufen

(1) Dieser AVV regelt das **Standard-Setup (Stufe 1 Standard)** mit Hosting in Deutschland und LLM-Verarbeitung über Anthropic Standard-API (US, abgesichert durch SCCs).

(2) Auf Anfrage stehen dem Mandanten zwei erweiterte Datenschutz-Stufen zur Verfügung:

- **Stufe 2 Premium EU-Datenraum:** EU-only LLM-Provider, optionale serverseitige PII-Maskierung, jährlicher Remote-Audit. Konditionen und Vertragsausgestaltung individuell auf Anfrage.
- **Stufe 3 Datensouverän:** Customer-On-Premise oder dediziertes EU-Hosting, Pflicht-PII-Maskierung vor LLM-Übergabe, Vor-Ort-Audit-Recht, Customer-Whitelist für Sub-Auftragsverarbeiter. Konditionen und Vertragsausgestaltung individuell auf Anfrage; Custom-Engineering erforderlich.

(3) Anfragen für Stufe 2 oder Stufe 3 sind über das Kontaktformular auf der FIP-Website zu richten. FIP unterbreitet daraufhin ein individuelles Vertragsangebot.

§ 10 Drittlandtransfer

(1) Im Rahmen des Standard-Setups (Stufe 1) findet ein **Drittlandtransfer in die USA** statt: FIP nutzt Anthropic, PBC (Sitz USA) als Sub-Auftragsverarbeiter für LLM-gestützte Auswertungen.

(2) Der Drittlandtransfer ist abgesichert durch **EU-Standardvertragsklauseln (SCCs) in der jeweils gültigen Fassung, insbesondere Modul 3 Processor-to-Processor für die FIP-Anthropic-Beziehung**, sowie einen **Transfer-Impact-Assessment (TIA)**, der dem Mandanten auf Anfrage zur Verfügung gestellt wird.

(3) Anthropic verpflichtet sich vertraglich, die übermittelten Daten **nicht zum Training eigener Modelle** zu verwenden (Standard-API-ToS) und die Daten innerhalb von **30 Tagen** nach API-Call zu löschen.

(4) Bei Stufe 2 und Stufe 3 findet kein Drittlandtransfer statt.

§ 11 Löschung und Rückgabe

(1) FIP löscht alle personenbezogenen Daten des Mandanten **innerhalb von 30 Kalendertagen** nach dem maßgeblichen Löschzeitpunkt oder gibt sie auf Verlangen des Mandanten zurück. Der maßgebliche Löschzeitpunkt ist:

- bei **Leistungsstufe 1 Diagnostik:** das Ende der Read-Only-Phase (6 Monate nach Integrity-Report-Übergabe);
- bei **Leistungsstufe 2 Erfolgshonorar** und **Leistungsstufe 3 Mandat:** das Ende der EDR-Survival-Frist von 90 Kalendertagen nach Vertragsende (vgl. AGB § 13 Abs. 5);
- beim **Potenzial-Check ohne Folge-Mandat:** das früheste der folgenden Ereignisse: Ergebnis-Call, Ablehnung eines Folge-Mandats durch den Mandanten, oder Ablauf von 30 Kalendertagen nach Datenübermittlung.

Bei Stufe 2 verkürzt sich die Löschfrist auf 14 Kalendertage, bei Stufe 3 auf 7 Kalendertage.

(2) Bestehende **gesetzliche Aufbewahrungspflichten** (insbesondere § 257 HGB, § 147 AO) bleiben unberührt; entsprechende Daten werden gesperrt und nach Ablauf der Aufbewahrungsfristen gelöscht.

(3) Technische Backup-Kopien werden nach den im normalen Backup-Lifecycle vorgesehenen Fristen überschrieben (in der Regel innerhalb von 30 Tagen nach Hauptlöschung).

(4) FIP bestätigt die Löschung in Textform.

§ 12 Unterstützung bei Betroffenenrechten

(1) FIP unterstützt den Mandanten bei der Beantwortung von Anfragen betroffener Personen nach Art. 15 bis 22 DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).

(2) **Reaktionsfristen:** FIP reagiert auf entsprechende Anfragen des Mandanten in der Regel innerhalb von **14 Kalendertagen**.

(3) **Aufwand:** In Stufe 1 ist je 1 Anfrage pro Mandat und Monat in der Vergütung inkludiert. Darüber hinausgehender Aufwand wird zum jeweils gültigen Stundensatz abgerechnet.

§ 13 Datenschutzverletzungen

(1) FIP meldet dem Mandanten **innerhalb von 24 Stunden** nach Kenntnisnahme alle Verletzungen des Schutzes personenbezogener Daten, die im Verantwortungsbereich von FIP eintreten.

(2) Die Meldung enthält, soweit verfügbar: Art der Verletzung, Kategorien und Anzahl der betroffenen Datensätze, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Gegenmaßnahmen.

(3) FIP unterstützt den Mandanten bei der Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und bei der Benachrichtigung betroffener Personen (Art. 34 DSGVO).

(4) FIP unterhält eine **Berufshaftpflicht- und Cyber-Versicherung** mit angemessenen Deckungssummen. Der jeweils aktuelle Versicherungsnachweis wird auf Anfrage offengelegt.

§ 14 Nachweise und Auditrecht

(1) FIP erteilt dem Mandanten auf schriftliche Anfrage Auskunft über die getroffenen technisch-organisatorischen Maßnahmen und stellt das nach Art. 30 Abs. 2 DSGVO geführte Verarbeitungsverzeichnis, die jeweils aktuelle Sub-Auftragsverarbeiter-Liste, den Versicherungsnachweis und geeignete weitere Nachweise auf Anforderung zur Verfügung.

(2) In Stufe 1 erfolgt die Kontrolle grundsätzlich durch Selbstauskunft und Bereitstellung der vorgenannten Nachweise. Ein **Vor-Ort-Audit** durch den Mandanten oder einen von ihm beauftragten neutralen Prüfer ist bei berechtigtem Anlass — insbesondere bei einem Datenschutzvorfall oder begründetem Verdacht einer wesentlichen Pflichtverletzung — nach angemessener Vorankündigung von mindestens zehn Werktagen zulässig.

(3) Die konkrete Audit-Form für erweiterte Datenschutz-Stufen wird im individuellen AVV nach § 9 vereinbart.

(4) Audits sind so durchzuführen, dass der Geschäftsbetrieb von FIP, die Sicherheit der Systeme, Geschäftsgeheimnisse und Rechte anderer Mandanten nicht unverhältnismäßig beeinträchtigt werden. Der Mandant und von ihm beauftragte Prüfer sind zur Vertraulichkeit zu verpflichten.

§ 15 Anonymisierungs-Klausel

(1) FIP darf die übermittelten Mandanten-Daten in **aggregierter und anonymisierter Form ohne Rückbezug auf einzelne Mandanten** zur Weiterentwicklung der eigenen Engine (Detection-Pattern, Konfidenz-Bewertung, Engine-Qualität) verwenden — konsistent mit AGB § 9 Abs. 5.

(2) **Trennlinie:** Die Anonymisierung selbst ist Verarbeitung im Auftrag und unterliegt diesem AVV. Erst nach **irreversibler Anonymisierung** (Token-Replacement, Aggregation, ausreichend hohe k-Werte pro Aggregat) verliert der Datensatz den Personenbezug und fällt aus dem DSGVO-Scope. Die Mindestparameter der Anonymisierung werden technisch dokumentiert und jährlich überprüft; FIP stellt dem Mandanten auf Anfrage eine abstrakte Beschreibung des Anonymisierungs-Konzepts ohne Offenlegung von Geschäftsgeheimnissen zur Verfügung.

(3) FIP verpflichtet sich, anonymisierte Datensätze **nicht zu re-identifizieren** — weder während der Mandatslaufzeit noch danach.

(4) Eine **Weitergabe anonymisierter Daten an Dritte** zum Training derer Modelle ist ausgeschlossen.

§ 16 Schlussbestimmungen

(1) **Anwendbares Recht und Gerichtsstand.** Es gilt das Recht der Bundesrepublik Deutschland; ausschließlicher Gerichtsstand ist Berlin.

(2) **Textform und Salvatorische Klausel.** Änderungen und Ergänzungen bedürfen der Textform (§ 126b BGB). Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) **Click-Wrap.** Dieser AVV kann durch elektronische Zustimmung im FIP-Portal geschlossen werden. Die zustimmende Person bestätigt, zur Vertretung des Mandanten berechtigt zu sein. Der vollständige AVV-Text wird vor Zustimmung als speicherbarer und druckbarer PDF-Snapshot bereitgestellt. Der Zustimmungs-Vorgang wird revisionssicher protokolliert (Name, geschäftliche E-Mail, Unternehmen, Rolle, Zeitstempel, IP-Adresse, Hashwert). Der Mandant erhält unverzüglich eine Bestätigungs-E-Mail mit Anhang des akzeptierten Vertragstextes. Eine **separate Bestätigungs-Checkbox** wird aus Nachweis- und Transparenzgründen eingesetzt.

(4) **Anlagen.** Folgende Anlagen sind Bestandteil dieses AVV jeweils in der zum Click-Wrap-Zeitpunkt gültigen Fassung:

- Anlage 1: TOMs-Anlage Stufe 1, Hash SHA-256: 0f324e71a839fb5a9a37fd1a4bc9f6ef37e9a23dc775e2f4f3da06a882d1399e
- Anlage 2: Sub-Auftragsverarbeiter-Liste, Hash SHA-256: ce213d96b740758596d7929a52646046b0249b1d7bc2413917189429be32f4fb

---

Bei schriftlichem Abschluss:

Ort, Datum: _____

Für **FIP** (Keysers Services UG (haftungsbeschränkt)): _____ Sven Keysers, Geschäftsführer

Für den **Mandanten** ([FIRMA]): _____ [NAME], [FUNKTION]

Bei Click-Wrap-Abschluss über das FIP-Portal entfällt dieser Unterschriften-Block (siehe § 16 Abs. 3).

Anlage 1 zum AVV — Technisch-organisatorische Maßnahmen (TOMs) Stufe 1 Standard

Keysers Services UG (haftungsbeschränkt) · Marke „Financial Integrity Partners" (“FIP”)
Stand: 2026-05-28 · **Version:** 1.0 · **Bezug:** AVV-Kundenfassung in der jeweils gültigen Fassung § 7

Diese Anlage beschreibt die technisch-organisatorischen Maßnahmen (TOMs) nach Art. 32 DSGVO für das **Standard-Setup (Stufe 1)**. Für Stufe 2 (Premium EU-Datenraum) und Stufe 3 (Datensouverän) gelten erweiterte Maßnahmen, die in individuellen AVV festgehalten werden.

---

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

1.1 Zutrittskontrolle (physischer Schutz)

Die Production-Infrastruktur wird bei der IONOS SE in Deutschland betrieben, einschließlich georedundanter Backup-Standorte innerhalb Deutschlands. IONOS unterhält ISO/IEC 27001-zertifizierte Rechenzentren mit mehrstufiger physischer Zutrittskontrolle, 24/7-Bewachung, Brandschutz, redundanter Stromversorgung und kontrollierter Klimatisierung gemäß Stand der Technik. FIP-Mitarbeiter haben keinen physischen Zutritt zu den Server-Räumen.

1.2 Zugangskontrolle (logischer Zugang)

- Zugriff auf Production-Systeme ausschließlich über **SSH mit Schlüssel-basierter Authentifizierung**; Password-Authentifizierung ist deaktiviert
- Privater SSH-Schlüssel verschlüsselt mit Passphrase, aufbewahrt im verschlüsselten Container
- Customer-Portal-Zugang über **Token-basierte Authentifizierung**; Tokens und PINs werden mit bcrypt (rounds=12) gehasht in der Datenbank gespeichert (kein Plain-Storage); Tokens sind zeitlich limitiert und an die Engagement-Lifecycle-Phase gebunden
- Failed-Login-Schutz mit automatischer IP-Sperre (fail2ban)
- Session-Bindung an Token-Gültigkeit; ungenutzte Sessions verfallen

1.3 Zugriffskontrolle (Berechtigungen)

- **Rollen-basiertes Zugriffsmodell:** FIP-Admin (Geschäftsführung), autorisierte Reviewer, Customer-User
- Customer sehen ausschließlich Daten **ihres eigenen Mandats** (Mandanten-Trennung auf DB-Ebene)
- FIP-interner Zugriff auf Customer-Daten ausschließlich durch autorisierte Reviewer für konkrete Support-/Analyse-Anfragen

- **Audit-Trail** aller Datenzugriffe und Status-Änderungen (User-ID, Timestamp, Aktion, Datensatz-ID), Retention 90 Tage rollend

1.4 Trennungskontrolle

- **Mandanten-Daten-Isolation** auf Datenbank-Ebene (Tenant-Filterung mit Engagement-ID-Gating)
- Trennung zwischen Production-, Staging- und Demo-Umgebung
- Demo-Mandant nutzt ausschließlich **FIP-eigene Beispieldaten**, keine Customer-PII
- Backup-Daten getrennt nach Mandant zugeordnet

1.5 Pseudonymisierung und Verschlüsselung

- **Transit-Verschlüsselung:** TLS 1.2+ (Let's Encrypt-Zertifikate, Traefik als Reverse Proxy) für alle Customer-Portal-Verbindungen und API-Calls
- **At-Rest-Verschlüsselung:** verschlüsseltes Storage auf Block-Device-Ebene (LUKS) für Customer-Daten-Partition; verschlüsselte Backups bei IONOS-Backup-Service (AES-256 georedundant DE)
- **Schlüssel-Management:** SSH-Schlüssel + Storage-Encryption-Keys getrennt verwaltet
- Pseudonymisierung sensibler Identifikatoren ist Stufe-3-Standard (Datensouverän); in Stufe 1 trägt der Mandant die Datenminimierungs-Verantwortung beim Export

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Datenübertragung an Sub-Auftragsverarbeiter (Anthropic) ausschließlich über **TLS 1.2+ mit API-Token-Authentifizierung**
- Logging aller Outbound-API-Calls inkl. Datenmenge und Empfänger (Retention 30 Tage rollend für Application-Logs, 90 Tage für Access-Logs)
- Customer-Daten verlassen die EU ausschließlich für LLM-Verarbeitung bei Anthropic (US), gesichert durch EU-Standardvertragsklauseln, insbesondere Modul 3 Processor-to-Processor für die FIP-Anthropic-Beziehung, Anthropic DPA und Transfer-Impact-Assessment (TIA)
- Datenminimierung im Engine-Code: nur erforderliche Daten-Snippets je LLM-Call, keine pauschalen Exporte

2.2 Eingabekontrolle

- **Audit-Trail-Protokollierung** aller Eingaben, Status-Änderungen und Löschungen im Mandanten-Portal mit User-ID, Timestamp, IP und Aktions-Typ
- Aufbewahrung Audit-Log: 90 Tage rollend
- Append-only-Strategie zur Manipulationssicherheit

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

3.1 Verfügbarkeit

- **Tägliche Backups** der Customer-Datenbank über den IONOS-Backup-Service (verschlüsselt, georedundant DE)

- Retention-Strategie für rollende Backups
- Monitoring der Infrastruktur durch IONOS rund um die Uhr; Anwendungs-Monitoring durch FIP

3.2 Wiederherstellbarkeit

- **Backup-Restore-Verfahren** dokumentiert; Restore-Tests erfolgen vor erstem produktiven Mandat sowie mindestens jährlich; Wiederherstellungszeit und Datenverlust-Fenster werden bei jedem Test gemessen und dokumentiert
- Bei Datenverlust: Customer-Benachrichtigung innerhalb 24 Stunden, soweit datenschutzrelevant

3.3 Resilienz

- Schutz vor DDoS-Angriffen durch IONOS-Edge-Filtering im Standard-Tarif
- Regelmäßige Security-Patches gemäß Stand der Technik
- Software-Dependencies werden via Renovate-Bot überwacht (CVE-Alerts)

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

4.1 Datenschutzmanagement

- **Datenschutz-Verantwortlicher:** Geschäftsführung des Unternehmens; die Bestellung eines externen Datenschutzbeauftragten erfolgt bei Überschreiten der Schwellenwerte des § 38 BDSG
- Interne Datenschutz-Policy
- Personal-Verpflichtung auf Vertraulichkeit nach Art. 28 Abs. 3 lit. b DSGVO für alle Verarbeitenden
- BYOD-Nutzungsvereinbarung mit den Verarbeitenden bei Nutzung privater Geräte
- **Verarbeitungsverzeichnis** nach Art. 30 Abs. 2 DSGVO geführt; pro Customer-Mandat automatisiert um einen Customer-Eintrag ergänzt

4.2 Incident-Response

- **Incident-Response-Plan** dokumentiert mit Meldeketten, Eskalations-Kontakten und E-Mail-Vorlagen für Customer-Information
- Meldekette: Detection → FIP-Geschäftsführung → Customer-Benachrichtigung innerhalb 24 Stunden → ggf. Aufsichtsbehörde innerhalb 72 Stunden
- Versicherungsschutz: FIP unterhält eine Berufshaftpflicht- und Cyber-Versicherung mit angemessenen Deckungssummen; Versicherungsnachweis auf Anfrage

4.3 Datenschutz-Folgenabschätzung (DSFA)

- Bei Bedarf wird ein generisches DSFA-Template für Stufe 1 bereitgestellt
- Für Stufe 2 und Stufe 3 erfolgt eine individuelle DSFA je Mandat

4.4 Code- und Sicherheits-Reviews

- **Pull-Request-basierte Code-Reviews** für sicherheitsrelevante Änderungen
- **Penetrations-Tests** durch externen Sicherheits-Dienstleister vor dem ersten Leistungsstufe-2- oder Mandat der Leistungsstufe 3 mit personenbezogenen

Echtdaten oder vor der erstmaligen Verarbeitung produktiver Mandantendaten eines Enterprise-Mandanten
- TOMs werden mindestens **jährlich überprüft** und bei Bedarf angepasst

4.5 Auftragnehmer-Kontrolle

- Sub-Auftragsverarbeiter werden vor Beauftragung auf DSGVO-Konformität geprüft
- Bestehende Sub-AVs werden jährlich auf weiterhin gültige DSGVO-Konformität überprüft
- AVV mit jedem Sub-Auftragsverarbeiter dokumentiert (IONOS DSGVO-Standard-AVV, Anthropic SCCs + Standard-API-ToS)

Ergänzende Hinweise

- Diese TOMs-Anlage ist **versionsfähig**: Änderungen werden dem Mandanten gemäß AVV § 7 Abs. 2 in Textform mitgeteilt.
- Bei Änderungen, die das Sicherheitsniveau **wesentlich verschlechtern**, hat der Mandant ein Sonderkündigungsrecht.
- Die TOMs sind als **Minimum-Standard** zu verstehen; FIP kann jederzeit über das beschriebene Niveau hinausgehende Maßnahmen ergreifen.
- Stufe 2 (Premium EU-Datenraum) ergänzt diese TOMs um EU-only-Garantie für LLM-Provider, optionale serverseitige PII-Maskierung und Remote-Audit-Recht. Stufe 3 (Datensouverän) ergänzt um Pflicht-PII-Maskierung, Vor-Ort-Audit, Air-Gapped Backups und Customer-spezifische Sub-AV-Whitelist.

Anlage 2 zum AVV — Sub-Auftragsverarbeiter-Liste

Keysers Services UG (haftungsbeschränkt) · Marke „Financial Integrity Partners" (“FIP”) Stand: 2026-06-03 · Version: 1.1 · Bezug: AVV-Kundenfassung in der jeweils gültigen Fassung § 8

Diese Anlage enthält die jeweils aktuelle Liste der von FIP eingesetzten Sub-Auftragsverarbeiter. Änderungen werden dem Mandanten mit 30 Tagen Vorlaufzeit in Textform mitgeteilt (vgl. AVV § 8 Abs. 2).

---

1. Aktuelle Sub-Auftragsverarbeiter (Stufe 1 Standard)

#	Sub-AV	Sitz / Datenstandort	Verarbeitungszweck	Verarbeitete Daten	Rechtsgrundlage / AVV
1	**IONOS SE**	Deutschland (Karlsruhe + georedundantes Backup)	Hosting Production-Server, Datenbank, SMTP-Versand	alle vom Mandanten übermittelten Daten	DSGVO-Standard-AVV von IONOS, aktiv
2	**Anthropic, PBC**	USA	LLM-gestützte Auswertung im Rahmen der Engine-Analyse (Claude API, Standard-Leistungsstufe)	aggregierte Buchungs- und Belegs-Inhalte, soweit für Finding-Generierung erforderlich	Anthropic Commercial Terms + Anthropic Data Processing Addendum (DPA) + EU-Standardvertragsklauseln (SCCs) **Modul 3 Processor-to-Processor** für die FIP-Anthropic-Beziehung (soweit im Einzelfall erforderlich zusätzlich

			Modul 2) + Anthropic Sub-Processor-Liste + Transfer-Impact-Assessment (TIA) + dokumentierte No-Training-Garantie und 30-Tage-Retention

1a. Technische Dienste ohne Zugriff auf Mandatsdaten

Diese Dienste verarbeiten keine personenbezogenen Mandatsdaten und werden nicht als Sub-Auftragsverarbeiter geführt; sie sind aus Transparenzgründen separat aufgeführt.

#	Dienst	Sitz	Zweck
1	**Internet Security Research Group (Let's Encrypt)**	USA (gemeinnützig)	Bereitstellung von TLS-Zertifikaten für analyse.keysers.de; rein technisch, kein Zugriff auf Mandatsinhalte

2. Verarbeitungs-Details Anthropic

- **Eingesetzte Modelle:** Claude (Opus, Sonnet, Haiku — Auswahl je nach Engine-Modul)
- **API-Leistungsstufe:** Standard (kein Modell-Training auf API-Inputs, vertraglich zugesichert)
- **Retention bei Anthropic:** maximal 30 Kalendertage (Anthropic-ToS)
- **Drittland-Absicherung:** EU-Standardvertragsklauseln (Modul 3 Processor-to-Processor); TIA dokumentiert die rechtlichen und technischen Maßnahmen
- **Datenminimierung:** Engine übermittelt nur die für die jeweilige Auswertung erforderlichen Datenfelder, keine pauschalen Buchungs-Exports

3. Backlog / Geprüft bei Aktivierung

Folgende Anbieter sind aktuell **nicht aktiv eingesetzt**, könnten aber bei Stack-Erweiterung relevant werden. Sie würden gemäß AVV § 8 Abs. 2 mit 30 Tagen Vorlauf angekündigt werden:

Anbieter	Auslöser für Aktivierung

Cloudflare (CDN/Edge)	Aktuell nicht vor IONOS geschaltet — würde Customer-Mitteilung erfordern, falls aktiviert
eSignature-Service (DocuSign, Skribble)	Aktivierung bei Engagement-Letter-Auto-Send (geplant; siehe Customer-Onboarding-Konzept Schritt 4)
Application-Monitoring (Sentry o.ä.)	Aktivierung wenn Application-Errors mit Customer-Identifikatoren extern geloggt werden sollen
Externer Mail-Service (SendGrid, Postmark)	Aktivierung bei Migration weg von IONOS-SMTP
Lead-Form-Provider (HubSpot, Plausible)	Aktivierung bei Wechsel von Eigen-Form auf externes Tool

4. Nicht Gegenstand dieses AVV

Anbieter für FIP-eigene Vertriebs-, Marketing- und Infrastruktur-Prozesse, die **keine Mandatsdaten** des Mandanten verarbeiten, fallen nicht unter diesen AVV. Diese Verarbeitungen erfolgen in eigener datenschutzrechtlicher Verantwortung von FIP und werden in den FIP-Datenschutzhinweisen auf der Website geregelt. Beispiele:

Anbieter	Zweck	Begründung
GitHub Inc.	Code-Hosting	kein Production-Daten-Touch, ausschließlich Quellcode
Docker Hub / GHCR	Container-Image-Hosting	kein Production-Daten-Touch
Apollo.io	Lead-Daten für FIP-eigenes Outreach (FIP als Verantwortlicher)	keine Customer-Mandatsdaten; eigene Datenschutzhinweise und Apollo-DPA gelten gesondert

5. Änderungs-Verfahren

(1) Bei Hinzufügen oder Wechsel eines Sub-Auftragsverarbeiters gilt **AVV § 8 Abs. 2**:

- Mitteilung in Textform an den Mandanten mit 30 Tagen Vorlaufzeit
- Widerspruchsrecht des Mandanten in Textform innerhalb der 30-Tage-Frist
- Im Widerspruchsfall: außerordentliches Kündigungsrecht des Mandanten

(2) Diese Liste wird **versioniert** geführt. Bei jeder Änderung wird die Versionsnummer hochgezählt und die Änderung dokumentiert.

(3) Der Mandant kann die jeweils aktuelle Sub-AV-Liste jederzeit über das FIP-Portal oder per Anfrage an **sven@keysers.de** abrufen.

Änderungs-Historie

Version	Datum	Änderung
1.0	2026-05-28	Initial-Version mit zwei Sub-AVs (IONOS, Anthropic) plus technischem Dienst (Let's Encrypt, kein Sub-AV)
1.1	2026-06-03	Versionsangleichung an AVV-Paket v1.1; Inhalt unverändert (IONOS + Anthropic)