Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO – zwischen dem Auftraggeber (Verantwortlicher) und AX1S / AIGOY (Auftragsverarbeiter)

AUFTRAGGEBER (VERANTWORTLICHER)

[Firma / Name]
[Straße, Nr.]
[PLZ, Ort], [Land]
vertreten durch: [Name]
nachfolgend „Auftraggeber“

AUFTRAGNEHMER (AUFTRAGSVERARBEITER)

Thomas Brandt, Einzelunternehmer
handelnd unter der Marke AX1S / AIGOY
AX1S c/o Clevver, Winterhuder Weg 29
22085 Hamburg, Deutschland
nachfolgend „Auftragnehmer“

§ 1 Gegenstand und Dauer

Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Bereitstellung der AIGOY-Plattform (AI Governance, Risk & Compliance). Die Laufzeit entspricht der des Hauptvertrags und endet mit dessen Beendigung.

---

§ 2 Art, Umfang und Zweck der Verarbeitung

Bereitstellung der AIGOY-Plattform und ihrer Module (u. a. KI-Inventar, Risk Management, Policy Management, Compliance Reporting, Board Portal, Training Hub, Whistleblowing) sowie KI-gestützte Vorbereitung von Richtlinien und Risikobewertungen durch den Compliance-CoWorker „Felix“ im Vier-Augen-Prinzip. Die Verarbeitung erfolgt ausschließlich zur Leistungserbringung und auf dokumentierte Weisung des Auftraggebers.

---

§ 3 Art der Daten und Kategorien betroffener Personen

Art der personenbezogenen Daten (typisch):

- Stamm-/Kontaktdaten (Name, dienstliche E-Mail, Abteilung, Rolle)
- Authentifizierungsdaten (verschlüsseltes Passwort, Login-Zeitstempel, Session-Token)
- Nutzungs- und Protokolldaten der Plattform (inkl. Audit-Trail)
- Schulungs-/Kompetenzdaten (Modulfortschritt, Nachweise)
- vom Auftraggeber eingestellte Inhaltsdaten (z. B. Richtlinien, Risiken, Meldungen)

Kategorien betroffener Personen: Beschäftigte, Führungskräfte und Organe des Auftraggebers, Plattform-Nutzer sowie ggf. Dritte, deren Daten der Auftraggeber im Rahmen seiner Compliance-Prozesse einstellt.

Besondere Kategorien (Art. 9 DSGVO) sind nicht Gegenstand der vertragsgemäßen Nutzung; ihre Einstellung obliegt allein dem Auftraggeber und ist zu vermeiden.

---

§ 4 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich gemäß Art. 28 Abs. 3 DSGVO insbesondere:

1. Daten ausschließlich auf dokumentierte Weisung des Auftraggebers zu verarbeiten (auch bei Drittlandbezug, soweit keine rechtliche Verpflichtung besteht).
2. zur Verarbeitung befugte Personen auf Vertraulichkeit zu verpflichten.
3. die nach Art. 32 DSGVO erforderlichen TOM umzusetzen (Anlage 1).
4. die Bedingungen für weitere Auftragsverarbeiter (Art. 28 Abs. 2 und 4) einzuhalten (§ 6, Anlage 2).
5. den Auftraggeber bei der Erfüllung der Betroffenenrechte (Art. 12–23) zu unterstützen.
6. den Auftraggeber bei den Pflichten aus Art. 32–36 (Sicherheit, Meldungen, DSFA) zu unterstützen.
7. Daten nach Verarbeitungsende nach Wahl des Auftraggebers zu löschen oder zurückzugeben (§ 10).
8. Nachweise bereitzustellen und Überprüfungen zu ermöglichen (§ 9).

---

§ 5 Technische und organisatorische Maßnahmen (TOM)

Es gelten die TOM nach Anlage 1 (Art. 32 DSGVO). Maßnahmen dürfen dem technischen Fortschritt angepasst werden, sofern das Schutzniveau nicht unterschritten wird.

---

§ 6 Unterauftragsverarbeiter

Der Auftraggeber genehmigt allgemein die in Anlage 2 genannten Unterauftragsverarbeiter. Der Auftragnehmer schließt mit ihnen Verträge nach Art. 28 DSGVO mit gleichwertigen Pflichten. Änderungen werden rechtzeitig mitgeteilt; der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Für Drittlandübermittlungen gelten Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) bzw. das EU-U.S. Data Privacy Framework.

§ 7 Rechte der betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber bei Anträgen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) und leitet unmittelbar an ihn gerichtete Anliegen unverzüglich weiter.

§ 8 Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden mit den nach Art. 33 DSGVO erforderlichen Informationen, damit der Auftraggeber seinen Pflichten nach Art. 33, 34 DSGVO nachkommen kann.

§ 9 Kontroll- und Nachweisrechte

Nachweise erfolgen vorrangig über geeignete Belege (z. B. SOC 2 Type II der eingesetzten Infrastruktur, Auditberichte, TOM-Dokumentation). Soweit erforderlich, ermöglicht der Auftragnehmer Überprüfungen mit angemessener Vorankündigung und ohne unverhältnismäßige Betriebsstörung.

§ 10 Löschung und Rückgabe

Nach Verarbeitungsende löscht oder übergibt der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten und vernichtet Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht. Die Löschung wird auf Wunsch bestätigt.

§ 11 Haftung

Die Haftung richtet sich nach Art. 82 DSGVO und dem Hauptvertrag.

§ 12 Schlussbestimmungen

Änderungen bedürfen der Textform. Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieser Vereinbarung dem Hauptvertrag vor. Es gilt deutsches Recht.

Ort, Datum – Auftraggeber	Ort, Datum – Auftragnehmer (AX1S / AIGOY)
Name / Funktion	Thomas Brandt

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

AIGOY ist in Deutschland entwickelt, wird in Deutschland gehostet und aus Deutschland betreut.

Schutzziel	Maßnahme
Vertraulichkeit	Verschlüsselung in Transit (TLS 1.2+) und at Rest (AES-256); Row Level Security (RLS); rollenbasierte Zugriffe (Least-Privilege).
Integrität	INSERT-only Audit-Trail; Vier-Augen-Approval-Cockpit – jede schreibende Aktion von Felix wird erst nach Freigabe wirksam.
Verfügbarkeit & Belastbarkeit	Regelmäßige Backups in der EU-Region; gehärtete Infrastruktur (Supabase / AWS eu-central-1 Frankfurt, SOC 2 Type II).
Datenresidenz	Verarbeitung/Speicherung in der EU (Frankfurt/DE). KI-Inferenz: keine Nutzung der Daten zu Trainingszwecken; EU-Inferenz (AWS Bedrock Frankfurt) in Vorbereitung.
Trennung	Logische Mandantentrennung (tenant_id) mit durchgesetzter RLS.
Auftragskontrolle	AVV (Art. 28) mit allen Unterauftragsverarbeitern; SCC/DPF für Drittlandbezug.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Standort	Leistung / Zweck	Hinweis
IONOS SE	Montabaur, Deutschland 🇩🇪	Webhosting	AVV Art. 28
Supabase Inc.	AWS eu-central-1, Frankfurt 🇩🇪 (EU)	Backend, Datenbank, Auth, Edge Functions	DPA Art. 28; SOC 2 Type II
Anthropic PBC	USA 🇺🇸	KI-Dienst (Modell Claude) für Analysen / CoWorker Felix	Kein Training auf Daten; SCC + EU-U.S. DPF; AVV Art. 28
Stripe Payments Europe, Ltd.	Dublin, Irland 🇮🇪 (EU)	Zahlungsabwicklung	nur Tarife Business / Enterprise

Stand: Mai 2026. Diese Vorlage dient als Ausgangspunkt und ersetzt keine Rechtsberatung. Vor Verwendung bitte an den Einzelfall anpassen und rechtlich prüfen lassen. Eine jeweils aktuelle Sub-Prozessor-Liste wird auf der Trust- & Sicherheitsseite

veröffentlicht.