CompliKI - Vereinbarung zur Auftragsverarbeitung (AVV)

AVV-Version 2026-06 - Stand 14. Juni 2026 - Anbieter: Christian Baltes, Baltes KI Solutions

Oeffentliche, generische Fassung gemaess Artikel 28 DSGVO (ohne kundenindividuelle Angaben).

Diese Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO wird Bestandteil des Vertrags zwischen dem Geschäftskunden (Verantwortlicher) und dem Anbieter von CompliKI (Auftragsverarbeiter). Sie regelt, wie der Anbieter personenbezogene Daten im Auftrag und nach Weisung des Kunden verarbeitet.

1. Parteien

Diese Vereinbarung wird geschlossen zwischen dem Kunden als Verantwortlichem im Sinne des Art. 4 Nr. 7 DSGVO und dem Anbieter als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO.

Auftragsverarbeiter ist:

2. Gegenstand und Dauer

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung und des Betriebs der Software-as-a-Service CompliKI für den Verantwortlichen.

Die Laufzeit dieser Vereinbarung entspricht der Lizenzlaufzeit des Hauptvertrags. Sie beginnt mit dessen Wirksamwerden und endet mit dessen Beendigung. Nach Beendigung des Vertrags werden die im Auftrag verarbeiteten Daten gemäß dem Löschkonzept und den in Abschnitt 8 beschriebenen Fristen zurückgegeben oder gelöscht.

3. Art, Umfang und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zum Zweck der Bereitstellung von CompliKI. CompliKI dient der strukturierten Erfassung, Erstbewertung, Organisation und Dokumentation der KI-Nutzung des Verantwortlichen im Hinblick auf die Anforderungen des EU AI Act (Verordnung (EU) 2024/1689).

Art und Umfang der Verarbeitung umfassen insbesondere:

- Erfassen, Speichern und Strukturieren von Angaben zu KI-Systemen,
- Erstellen, Versionieren und Exportieren von Compliance-Dokumentation,
- Verwalten von Nutzerkonten und Zugriffsrechten,
- Protokollieren sicherheitsrelevanter Vorgänge in einem Audit-Trail.

Die Verarbeitung erfolgt weisungsgebunden und nur zu den vereinbarten Zwecken. Eine Nutzung der Daten zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

4. Kategorien betroffener Personen und Daten

Von der Verarbeitung sind folgende Kategorien betroffener Personen erfasst:

- Mitarbeitende und Nutzer des Verantwortlichen mit einem Nutzerkonto in CompliKI,
- natürliche Personen, die in den vom Verantwortlichen eingegebenen Compliance-Inhalten benannt werden (z. B. als Verantwortliche oder Ansprechpartner eines KI-Systems).

Verarbeitet werden insbesondere folgende Datenkategorien:

- Stamm- und Kontaktdaten der Nutzerkonten (Name, E-Mail-Adresse, Rolle),
- Anmelde- und Zugriffsdaten in technisch erforderlichem Umfang,

- vom Verantwortlichen eingegebene Compliance-Inhalte zu KI-Systemen (Beschreibungen, Einstufungen, Bewertungen, Dokumente),

- technische Protokolldaten des Audit-Trails.

Der Verantwortliche entscheidet eigenständig über die Inhalte, die er in CompliKI eingibt. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sollen nur eingegeben werden, soweit dies für den jeweiligen Zweck erforderlich ist.

5. Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter setzt nach dem Stand der Technik geeignete technische und organisatorische Maßnahmen ein, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Hierzu gehören insbesondere:

- Verschlüsselte Übertragung: Transportverschlüsselung der Datenübertragung über TLS.

- Hosting in Deutschland: Betrieb der Kernanwendung auf Servern in Deutschland (STRATO).

- Zugriffskontrolle: rollenbasierte Zugriffsrechte und gesicherte Authentifizierung der Nutzerkonten.

- Mandantentrennung: logische Trennung der Kundendaten über eine eindeutige Mandantenkennung (tenant_id).

- Audit-Trail: hash-verkettete Protokollierung sicherheitsrelevanter Vorgänge.

- Backups: regelmäßige Datensicherungen mit definierter Aufbewahrung.

- Löschkonzept: dokumentierte Lösch- und Aufbewahrungsfristen für produktive Daten und Sicherungen.

6. Unterauftragnehmer (Subprozessoren)

Der Auftragsverarbeiter setzt zur Erbringung der Leistung sorgfältig ausgewählte Unterauftragnehmer ein. Die folgende Übersicht gibt den aktuellen Stand wieder:

Dienstleister	Zweck	Standort	Drittlandbezug	Schutzmechanismus
STRATO AG	Hosting der Kernanwendung (Compute, Storage)	Deutschland	nein	-
Stripe Payments Europe Ltd.	Zahlungsabwicklung	Irland (EU)	möglicher Zugriff durch Stripe Inc. (USA)	EU-Standardvertragsklauseln (SCC), DPA
united-domains AG	Versand transaktionaler E-Mails (SMTP)	Deutschland	nein	-
Anthropic PBC	KI-Co-Pilot (Claude), nur bei Nutzung der KI-Funktionen in Professional/Enterprise	USA	ja (Drittland)	EU-Standardvertragsklauseln (SCC), DPA
PostHog	Pseudonyme Reichweiten- und Nutzungsanalyse, nur nach Einwilligung	EU-Hosting (Frankfurt)	möglicher Zugriff durch PostHog Inc. (USA)	EU-Standardvertragsklauseln (SCC)

Ein gesonderter Dienstleister für Monitoring oder Fehler-Tracking wird derzeit nicht eingesetzt.

Der Verantwortliche wird über Änderungen im Bestand der Unterauftragnehmer informiert und kann diesen widersprechen.

7. Rechte des Verantwortlichen und Pflichten des Auftragsverarbeiters

Der Verantwortliche bleibt für die Rechtmäßigkeit der Verarbeitung verantwortlich und erteilt dem Auftragsverarbeiter Weisungen zur Verarbeitung. Der Auftragsverarbeiter verpflichtet sich insbesondere:

- Weisungsbindung: Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen.

- Vertraulichkeit: Verpflichtung der mit der Verarbeitung befassten Personen auf Vertraulichkeit.

- Unterstützung: Unterstützung des Verantwortlichen bei der Erfüllung von Betroffenenrechten (Art. 12-23 DSGVO) sowie bei Datenschutz-Folgenabschätzungen (Art. 35-36 DSGVO).

- Meldepflichten: unverzügliche Information des Verantwortlichen über Verletzungen des Schutzes personenbezogener Daten.

- Nachweis: Bereitstellung der zum Nachweis der Einhaltung erforderlichen Informationen und Ermöglichung von Überprüfungen.

8. Löschung und Rückgabe

Nach Beendigung des Vertrags werden die im Auftrag verarbeiteten Daten nach Wahl des Verantwortlichen zurückgegeben oder gelöscht. Es gelten die folgenden Fristen:

- Produktive Compliance-Inhalte werden spätestens 30 Tage nach Ende der Lizenz aus den produktiven Systemen gelöscht.

- Sicherungskopien werden innerhalb weiterer 90 Tage bereinigt.

Gesetzliche Aufbewahrungspflichten bleiben unberührt. Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen (z. B. Rechnungsdaten), werden erst nach Ablauf der jeweils geltenden Frist gelöscht und bis dahin in der Verarbeitung eingeschränkt.

Weitere Regelungen ergeben sich aus den AGB (§ 11 Datenschutz und Auftragsverarbeitung) sowie aus der Datenschutzerklärung.

Stand: Juni 2026 Letzte Aktualisierung: 14.06.2026 AVV-Version: 2026-06