Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Fassung: September 2026

1. Vertragsparteien

Dieser Auftragsverarbeitungsvertrag („AVV“) wird geschlossen zwischen:

Name des Kunden	
Adresse des Kunden	

und AITAS Technologies. Der Auftraggeber und der Auftragnehmer werden nachfolgend gemeinsam „Parteien“ genannt. Der vorliegende AVV wird von der oder dem bevollmächtigten Vertreter der jeweiligen Partei akzeptiert und vereinbart.

AITAS Technologies	**Kunde**
Name: Jannik Wiessler	Name:
Funktion: Autorisierter Unterzeichner	Funktion:
Unterschrift:	Unterschrift:
Datum:	Datum:

2. Gegenstand, Rangfolge und Einordnung

Der Auftragnehmer stellt dem Auftraggeber die Plattform Coveniq AI bereit. Bestandteil der Plattform ist ein Privacy Guard, der Inhalte vor einer möglichen Weitergabe an angebundene KI-Modelle analysiert und erkannte personenbezogene Angaben durch neutrale Platzhalter ersetzt. Die Verarbeitung erfolgt im Auftrag des Auftraggebers.

Dieser AVV ergänzt den jeweiligen Hauptvertrag oder die sonstigen Nutzungsbedingungen. Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieses AVV vor, soweit sie die Verarbeitung personenbezogener Daten im Auftrag betreffen.

Die Regelungen dieses AVV gelten unmittelbar für den laufenden Betrieb, soweit keine abweichenden produktspezifischen Anlagen vereinbart werden.

3. Rollen der Parteien

1. Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO für die personenbezogenen Daten, die er oder seine Nutzer in Coveniq AI eingeben, hochladen oder dort verarbeiten lassen.
2. Der Auftragnehmer verarbeitet personenbezogene Daten als Auftragsverarbeiter ausschließlich im Rahmen dieses AVV und nach dokumentierter Weisung des Auftraggebers.
3. Die Verantwortung für Rechtmäßigkeit, Zweckbestimmung, Transparenzpflichten gegenüber betroffenen Personen und Auswahl der in Coveniq AI eingegebenen Daten verbleibt beim Auftraggeber.

4. Eine Verarbeitung durch den Auftragnehmer zu eigenen Zwecken findet nicht statt, soweit sie nicht in diesem AVV, im Hauptvertrag oder in einer gesonderten Vereinbarung ausdrücklich beschrieben ist.

4. Gegenstand, Dauer, Art und Zweck der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung, der Betrieb und die technische Absicherung von Coveniq AI einschließlich Privacy Guard, Benutzerverwaltung, Prompt-Verarbeitung, Antwortgenerierung, technischer Protokollierung, Support und Fehleranalyse.

Die Verarbeitung erfolgt für die Dauer des jeweiligen Nutzungs- oder Vertragsverhältnisses einschließlich geordneter Nachlauf- und Löschfristen.

Die Art der Verarbeitung umfasst insbesondere:

- das Erheben, Erfassen, Organisieren und Ordnen personenbezogener Daten,
- das Speichern, Auslesen und Abfragen personenbezogener Daten,
- das Verwenden, Übermitteln, Abgleichen und Einschränken personenbezogener Daten,
- das Löschen und Vernichten personenbezogener Daten, soweit dies für den Betrieb der Plattform erforderlich ist.

Die Zwecke der Verarbeitung umfassen insbesondere:

- die KI-gestützte Verarbeitung von Nutzeranfragen,
- die Pseudonymisierung beziehungsweise Maskierung personenbezogener Angaben über den Privacy Guard,
- die Rückübersetzung von Platzhaltern in der Antwortdarstellung,
- die Anzeige von KI-generierten Antworten,
- die Verwaltung von Nutzerkonten,
- die Gewährleistung der Sicherheit der Plattform,
- Support, Fehlerbehebung und technische Analyse,
- die Abrechnung, soweit diese im jeweiligen Nutzungskontext einschlägig ist.

Personenbezogene Daten des Auftraggebers werden nicht zum Training eigener oder fremder KI-Modelle verwendet, sofern dies nicht ausdrücklich gesondert vereinbart wurde. Für die eingesetzten Modellanbieter ist darüber hinaus Zero Data Retention vereinbart und konfiguriert; Einzelheiten regelt die Anlage „Unterauftragsverarbeiter“.

5. Kategorien personenbezogener Daten

Je nach Nutzung können insbesondere folgende Daten verarbeitet werden:

1. Benutzer- und Kontodaten: Name, geschäftliche E-Mail-Adresse, Organisationszugehörigkeit, Rollen, Login- und Nutzungsdaten.
2. Inhaltsdaten: Prompts, Chatverläufe, hochgeladene Dateien, Auszüge aus Dokumenten, E-Mails, Protokollen, Verwaltungs-, Kunden-, Projekt- oder Geschäftsvorgängen.
3. Kommunikationsdaten: Supportanfragen, Rückmeldungen, technische Fehlermeldungen.
4. Technische Daten: IP-Adresse, Zeitstempel, Session-IDs, Geräte- und Browserinformationen, Protokoll- und Sicherheitsereignisse.

5. Durch den Privacy Guard erkannte Datenarten: Namen, E-Mail-Adressen, Telefonnummern, Anschriften, Identifikationsnummern, Datumsangaben, Organisations- und Rollenbezüge sowie weitere kontextabhängig erkennbare personenbezogene Angaben.
6. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, etwa Gesundheitsdaten, religiöse oder politische Angaben, sollen nur verarbeitet werden, wenn dies vom Auftraggeber ausdrücklich freigegeben und fachlich erforderlich ist.

6. Kategorien betroffener Personen

1. Nutzerinnen und Nutzer der Plattform beim Auftraggeber, insbesondere Mitarbeitende, Administratoren und berechtigte externe Personen.
2. Personen, deren Daten durch den Auftraggeber in Coveniq AI verarbeitet werden, zum Beispiel Kunden, Bürgerinnen und Bürger, Interessenten, Lieferanten, Geschäftspartner, Bewerber, Seminarteilnehmende, Schülerinnen und Schüler oder sonstige Dritte.
3. Kontaktpersonen im Rahmen von Support, Vertragsabwicklung und Administration.

7. Weisungen des Auftraggebers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern keine gesetzliche Pflicht zur Verarbeitung besteht.
2. Die Nutzung der Plattform durch berechtigte Nutzer des Auftraggebers, insbesondere das Eingeben von Prompts, Hochladen von Dateien, Abrufen von Antworten und Konfigurieren von Einstellungen, gilt als dokumentierte Weisung zur jeweiligen Verarbeitung.
3. Weisungen können in Textform erteilt werden. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
4. Hält der Auftragnehmer eine Weisung für rechtswidrig oder technisch risikobehaftet, weist er den Auftraggeber hierauf hin. Die Durchführung der Weisung kann ausgesetzt werden, soweit dies zum Schutz personenbezogener Daten erforderlich ist.

8. Vertraulichkeit und Zugriffsbeschränkung

1. Der Auftragnehmer stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Zugriffe auf personenbezogene Daten des Auftraggebers werden auf Personen beschränkt, die diese Zugriffe für Betrieb, Sicherheit, Support oder Fehleranalyse benötigen.
3. Produktivdaten werden nicht für interne Demonstrationen, Schulungen oder Entwicklungstests verwendet, sofern dies nicht zuvor anonymisiert oder gesondert vereinbart wurde.

9. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen („TOMs“), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die TOMs sind in der Anlage „Technische und organisatorische Maßnahmen“ beschrieben und können im Rahmen technischer Weiterentwicklung angepasst werden, sofern das Schutzniveau insgesamt nicht unterschritten wird.

Der Privacy Guard ist eine zusätzliche technische Schutzmaßnahme zur Reduktion der Offenlegung personenbezogener Daten gegenüber angebundenen KI-Modellen. Eine vollständige Erkennung sämtlicher personenbezogener oder vertraulicher Informationen kann technisch nicht garantiert werden.

10. Unterauftragsverarbeiter

1. Der Auftragnehmer darf weitere Auftragsverarbeiter nur mit vorheriger gesonderter oder allgemeiner Genehmigung des Auftraggebers einsetzen.
2. Der Auftraggeber erteilt eine allgemeine Genehmigung zum Einsatz der in der Anlage „Unterauftragsverarbeiter“ genannten Dienstleister.
3. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen bei Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mit angemessener Frist. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.
4. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich mindestens in dem Umfang, der für diesen AVV erforderlich ist.

11. Drittlandübermittlungen

Eine Übermittlung personenbezogener Daten in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der DSGVO erfüllt sind. Etwaige Drittlandübermittlungen werden in der Anlage „Unterauftragsverarbeiter“ beschrieben.

Soweit angebundene KI-Modelle oder sonstige Dienstleister außerhalb der EU oder des EWR eingesetzt werden, werden geeignete Garantien vereinbart, zum Beispiel Angemessenheitsbeschluss, EU-Standardvertragsklauseln und ergänzende Schutzmaßnahmen, soweit erforderlich.

Soweit der Privacy Guard personenbezogene Angaben durch Platzhalter ersetzt, werden Originalwerte und Re-Identifikationsmapping nicht an externe KI-Modellanbieter übermittelt, sofern dies nicht ausdrücklich abweichend vereinbart ist.

12. Unterstützung bei Betroffenenrechten

1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen bei der Beantwortung von Anfragen betroffener Personen, insbesondere zu Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.
2. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet der Auftragnehmer die Anfrage an den Auftraggeber weiter, sofern eine Zuordnung möglich ist, und beantwortet die Anfrage nicht eigenständig, soweit nicht gesetzlich erforderlich.
3. Der Auftraggeber bleibt für die inhaltliche Beurteilung und fristgerechte Erfüllung von Betroffenenrechten verantwortlich.

13. Datenschutzverletzungen und Sicherheitsvorfälle

1. Der Auftragnehmer informiert den Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden nach Bekanntwerden, über Verletzungen des Schutzes personenbezogener Daten, soweit Daten des Auftraggebers betroffen sind.

2. Die Meldung enthält, soweit verfügbar, Art des Vorfalls, betroffene Daten und Personen, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen sowie eine Kontaktstelle.
3. Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen Umfang bei dessen Melde- und Benachrichtigungspflichten.

14. Löschung und Rückgabe

1. Nach Beendigung der Verarbeitungsleistungen löscht der Auftragnehmer personenbezogene Daten des Auftraggebers oder gibt sie nach Wahl des Auftraggebers zurück, sofern keine gesetzliche Speicherpflicht besteht.
2. Technische Backups werden im Rahmen des regulären Backup-Zyklus überschrieben.
3. Der Auftragnehmer dokumentiert die Löschung oder Rückgabe auf angemessene Weise.

15. Kontrollrechte und Nachweise

1. Der Auftragnehmer stellt dem Auftraggeber die zur Prüfung der Einhaltung dieses AVV erforderlichen Informationen in angemessenem Umfang zur Verfügung.
2. Nachweise können insbesondere durch TOM-Beschreibung, Sicherheitskonzepte, Selbstauskünfte, Auditberichte oder vergleichbare Dokumentation erbracht werden.

16. Unterstützung bei Datenschutz-Folgenabschätzung

Soweit für die Nutzung von Coveniq AI durch den Auftraggeber eine Datenschutz-Folgenabschätzung oder Konsultation einer Aufsichtsbehörde erforderlich ist, unterstützt der Auftragnehmer den Auftraggeber mit den ihm verfügbaren Informationen zu Verarbeitung, TOMs, Unterauftragsverarbeitern und Privacy-Guard-Funktionalität.

17. Änderungen der Plattform und Weiterentwicklung

Coveniq AI kann funktional und technisch weiterentwickelt werden. Änderungen, die das Datenschutzniveau wesentlich beeinflussen, insbesondere neue Kategorien von Unterauftragsverarbeitern, neue Drittlandübermittlungen oder wesentliche Änderungen der Privacy-Guard-Logik, werden dem Auftraggeber in angemessener Form mitgeteilt.

18. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses AVV bedürfen der Textform, soweit keine strengere gesetzliche Form vorgeschrieben ist.
2. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
3. Es gilt das Recht der Bundesrepublik Deutschland, soweit keine zwingenden datenschutzrechtlichen Regelungen entgegenstehen.

Anlage A: Beschreibung der Verarbeitung

Feld	Beschreibung
Produkt	Coveniq AI
Funktionen	KI-Chat, Dokument- und Textverarbeitung, Privacy Guard, Prompt-Pseudonymisierung, Antwort-Rückübersetzung, Nutzer- und Rollenverwaltung, Support.
Speicherorte	Frankfurt, Deutschland
Speicherdauer	Bis zur Beendigung des Vertrags oder jederzeit bis zur Löschung durch den Kunden
Speicherdauer Logs	30 Tage
KI-Modellanbieter	Eingesetzt: OpenAI und Anthropic, jeweils mit Zero Data Retention. Vorsorglich benannt, aber nicht freigeschaltet: Perplexity AI, Gamma AI, Mistral AI, KI-Modelle über AWS Bedrock. Vor einer Freischaltung werden Anbieter-AVV, Verarbeitungsort und Drittlandgarantien geprüft und diese Anlage aktualisiert.