Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Dieser Vertrag gilt zwischen dem Kunden des Good Ads Copilot (Verantwortlicher, nachfolgend „Kunde“) und Nick Adamidis, Birther Straße 131, 42549 Velbert (Auftragsverarbeiter, nachfolgend „Anbieter“). Er ist Bestandteil der AGB (§ 9) und wird mit der Zustimmung zu den AGB vereinbart. Eine unterschriebene Fassung schicken wir auf Wunsch per E-Mail.

§ 1 Gegenstand und Dauer

(1) Der Anbieter verarbeitet personenbezogene Daten im Auftrag des Kunden, soweit das für die Leistungen des Good Ads Copilot nach den AGB nötig ist: Analyse, Überwachung und Optimierung des Google-Ads-Kontos und der vom Kunden verbundenen Google-Dienste, KI-Assistent „Neo“, Berichte, Hinweise und das Ausführen vom Kunden bestätigter Änderungen.

(2) Der Vertrag läuft so lange wie der Nutzungsvertrag (einschließlich Testphase) und endet mit ihm. Pflichten zur Löschung und Rückgabe (§ 11) gelten darüber hinaus.

§ 2 Art und Zweck der Verarbeitung

Erheben über Schnittstellen von Google, Speichern, Auswerten, Zusammenfassen durch KI, Anzeigen im Cockpit, Versenden von Berichten und Hinweisen, Ausführen bestätigter Änderungen, Löschen. Zweck ist allein die Erbringung der vertraglichen Leistungen. Eine Nutzung für eigene Zwecke des Anbieters, für Werbung oder zum Training von KI-Modellen findet nicht statt.

§ 3 Art der Daten und Kategorien betroffener Personen

Die Einzelheiten stehen in Anlage 1. Betroffen sind vor allem Nutzer des Kundenkontos, Personen, die bei Google nach Angeboten des Kunden suchen (Suchbegriffe), Kunden und Interessenten des Kunden (z. B. Bewertungen im Unternehmensprofil) sowie Ansprechpartner, deren Daten in Anzeigen, Produktdaten oder Einstellungen des Kunden stehen.

§ 4 Weisungen

(1) Der Anbieter verarbeitet die Daten nur auf dokumentierte Weisung des Kunden. Weisungen sind dieser Vertrag, die AGB und die Bestätigungen des Kunden im Cockpit (z. B. „Änderung ausführen“, „Dienst trennen“). Weitere Weisungen erteilt der Kunde in Textform an kontakt@good-ads-copilot.de.

(2) Hält der Anbieter eine Weisung für rechtswidrig, weist er den Kunden unverzüglich darauf hin und darf die Ausführung bis zur Klärung aussetzen. Eine Verarbeitung aufgrund gesetzlicher Pflichten teilt der Anbieter vorher mit, soweit das Gesetz es erlaubt.

§ 5 Pflichten des Anbieters

(1) Der Anbieter verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit, soweit sie nicht gesetzlich zur Verschwiegenheit verpflichtet sind.

(2) Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO aus Anlage 2 und passt sie dem Stand der Technik an. Das Schutzniveau darf dabei nicht sinken.

(3) Er unterstützt den Kunden mit den ihm vorliegenden Informationen bei Anfragen betroffener Personen (Art. 12–23 DSGVO) und bei den Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation).

(4) Eine Verletzung des Schutzes personenbezogener Daten meldet er dem Kunden unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie vorliegen.

(5) Daten verarbeitet er ausschließlich in Rechenzentren in der Europäischen Union (Frankfurt am Main). Übermittlungen in Drittländer erfolgen nur über die Unterauftragsverarbeiter aus Anlage 3 und nur auf

Grundlage von Art. 44 ff. DSGVO (Angemessenheitsbeschluss zum EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln).

(6) Mitarbeiter des Anbieters sehen Daten des Kunden nur, wenn der Kunde um Hilfe bittet, wenn er eingewilligt hat, wenn es für Sicherheit oder Missbrauchsabwehr nötig ist oder wenn das Gesetz es verlangt. Jede Einsicht wird protokolliert.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde erlaubt den Einsatz der Unterauftragsverarbeiter aus Anlage 3. Der Anbieter schließt mit ihnen Verträge, die diesem Vertrag entsprechende Datenschutzpflichten enthalten.

(2) Neue oder geänderte Unterauftragsverarbeiter teilt der Anbieter mindestens vier Wochen vorher in Textform mit. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen; können sich die Parteien nicht einigen, darf der Kunde den Nutzungsvertrag zum Zeitpunkt des Wechsels kündigen.

(3) Keine Unterauftragsverarbeitung sind Leistungen, die der Kunde selbst bei Dritten nutzt und mit dem Dienst verbindet (z. B. sein Google-Ads-Konto, Merchant Center, Tag Manager, Google Analytics, Search Console, Unternehmensprofil). Für diese Konten bleibt das Vertragsverhältnis zwischen dem Kunden und Google maßgeblich.

§ 7 Rechte und Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und die Rechte der betroffenen Personen verantwortlich (z. B. Hinweis auf die Nutzung des Dienstes in seiner eigenen Datenschutzerklärung).

(2) Der Kunde darf sich von der Einhaltung dieses Vertrags überzeugen. Vorrangig genügen Auskünfte und Nachweise des Anbieters in Textform; Prüfungen vor Ort sind nach rechtzeitiger Anmeldung zu üblichen Geschäftszeiten und ohne Störung des Betriebs möglich. Kosten trägt jede Partei selbst.

§ 8 Löschung und Rückgabe

(1) Nach Ende des Nutzungsvertrags löscht der Anbieter die Daten des Kunden innerhalb von 30 Tagen, soweit keine gesetzliche Aufbewahrungspflicht besteht (z. B. Rechnungen). Auf Wunsch stellt er dem Kunden vorher eine Kopie der gespeicherten Daten in einem gängigen Format zur Verfügung.

(2) Über Google-Dienste gelesene Daten löscht der Anbieter sofort, wenn der Kunde den Dienst trennt, und unabhängig davon spätestens nach 30 Tagen.

(3) Datensicherungen werden nicht gezielt bereinigt; die Daten verschwinden mit dem Ablauf der Sicherungen (Anlage 2). Bis dahin bleiben sie verschlüsselt und werden nicht verarbeitet.

§ 9 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln der AGB.

(2) Bei Widersprüchen geht dieser Vertrag den AGB vor, soweit es um den Schutz personenbezogener Daten geht. Änderungen bedürfen der Textform. Es gilt deutsches Recht; Gerichtsstand wie in den AGB.

Anlage 1 – Daten und betroffene Personen

- Konto und Nutzer: Name, E-Mail-Adresse, Firmenname, Anmelde- und Sitzungsdaten, Einstellungen, Zustimmungen.
- Google-Ads-Daten: Kampagnen, Anzeigengruppen, Anzeigentexte, Keywords, Suchbegriffe, die Personen bei Google eingegeben haben, Kosten, Klicks, Impressionen, Conversions, Standort- und Zielgruppen-Einstellungen, Zielseiten.
- Merchant Center (wenn verbunden): Produktdaten (Titel, Beschreibung, Merkmale, Kategorie, Kennungen, Bild-Adresse, Preis, Labels), Produktstatus, Kontohinweise, Leistung je Produkt.

- Tag Manager, Google Analytics, Search Console (wenn verbunden): Konten, Container, Tags, Trigger, Mess-IDs, Schlüsselereignisse, zusammengefasste Besuchs- und Suchzahlen, Suchanfragen, Sitemaps.
- Unternehmensprofil (wenn verbunden): Standortdaten (Name, Telefonnummern, Öffnungszeiten, Kategorie, Website) sowie Bewertungen mit Sterne-Wertung, Text, Datum, Name der bewertenden Person und Antworten.
- Website des Kunden: öffentlich erreichbare Inhalte, die der Dienst für Empfehlungen liest.
- Kommunikation: Chatverläufe mit dem KI-Assistenten, Support-Anfragen, Hinweise, Berichte.
- Protokolle: bestätigte Änderungen, Rücknahmen, technische Betriebsprotokolle.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nicht gezielt verarbeitet. Der Kunde stellt sicher, dass er solche Daten nicht in Chats oder Anzeigen einträgt.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- Rechenzentrum: Server bei DigitalOcean in Frankfurt am Main; physischer Zutritt nach den Sicherheitsstandards des Hosters.
- Zugang zum Server: Anmeldung nur mit SSH-Schlüssel, Passwort-Anmeldung abgeschaltet; Firewall lässt nur SSH, HTTP und HTTPS zu; automatische Sperre nach wiederholten Fehlversuchen (fail2ban); automatische Sicherheitsupdates des Betriebssystems.
- Trennung: eigener Systemnutzer und eigener Dienst je Anwendung; die Anwendung lauscht nur intern und ist nur über den Webserver erreichbar; Datenbankdateien sind nur für den Dienst lesbar; der Dienst läuft mit eingeschränkten Rechten (u. a. schreibgeschützte Systembereiche).
- Zugriff in der Anwendung: Rollen (Kunde, Administrator) mit serverseitiger Prüfung; strikte Trennung der Kundenkonten, regelmäßig automatisch getestet; Passwörter nur als Hash (PBKDF2-SHA256, 200.000 Runden); Zwei-Faktor-Anmeldung für Administratoren; serverseitige Sitzungen, Cookies nur über HTTPS und nicht per Skript lesbar; Begrenzung von Anmeldeversuchen; Schutz gegen fremde Formular-Absendungen (Herkunftsprüfung).
- Verschlüsselung: Übertragung nur per TLS (HTTPS mit HSTS); Zugangsschlüssel zu Google und Zwei-Faktor-Geheimnisse verschlüsselt in der Datenbank (eigener Schlüssel außerhalb der Datenbank); Datensicherungen verschlüsselt, der Schlüssel zum Entschlüsseln liegt nicht auf dem Server.
- Einsicht durch Mitarbeiter: nur unter den Bedingungen aus § 5 Abs. 6; jede Kundenansicht durch Administratoren wird protokolliert.

Integrität

- Änderungen in Konten des Kunden nur nach Vorschau und Bestätigung; Freigabe je Dienst und je Kunde schaltbar; Probelauf ohne Änderung, wo Google ihn anbietet.
- Jede bestätigte Änderung wird mit Zeitpunkt und Login protokolliert (Aufbewahrung 3 Jahre) und lässt sich, soweit möglich, zurücknehmen.
- Schutz des KI-Assistenten gegen eingeschleuste Anweisungen in Daten (z. B. in Suchbegriffen, Bewertungen oder Websites), regelmäßig mit Angriffs-Tests geprüft; Prüfung von Zahlen in KI-Antworten gegen die echten Daten.
- Abruf fremder Websites nur an öffentliche Adressen (Schutz gegen Zugriffe auf interne Systeme).

Verfügbarkeit und Belastbarkeit

- Nächtliche, verschlüsselte Sicherung der Datenbank mit Integritätsprüfung (Aufbewahrung 14 Tage); zusätzliche Kopie vor jedem Software-Update (in der Regel 30 Tage); Sicherungen des gesamten Servers durch den Hoster.
- Software-Updates nur über einen festen Ablauf mit automatischen Tests, Rauchtest im Betrieb und automatischer Rücknahme bei Fehlern.

– Tägliche Selbsttests, Fehler- und Kostenüberwachung mit Hinweisen an das Team; Begrenzung von Abrufen bei Google und der KI.

Löschung und Datensparsamkeit

– Feste Löschfristen (siehe Datenschutzerklärung Ziffer 12), automatische Löschläufe; Zugriffsprotokolle des Webservers 14 Tage, Betriebsprotokolle 30 Tage.
– Über Google-Dienste gelesene Daten: Löschung beim Trennen sofort, sonst spätestens nach 30 Tagen; Löschprotokoll ohne Inhalte.
– Nach Löschung eines Kontos bleibt im Änderungsprotokoll kein Login-Name zurück (Pseudonymisierung).

Regelmäßige Überprüfung

– Automatische Tests bei jedem Software-Update (u. a. Rechte je Rolle und Route, Trennung der Kundenkonten, Löschung), wiederkehrende Sicherheits- und Rechtsprüfungen mit dokumentierten Ergebnissen.

Anlage 3 – Unterauftragsverarbeiter

– DigitalOcean, LLC, 105 Edgeview Drive, Suite 425, Broomfield, CO 80021, USA — Hosting (Server in Frankfurt am Main, Deutschland). Drittland-Absicherung: EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln.
– Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, bzw. Google LLC, USA — Gemini-API (KI-Auswertung, Assistent „Neo", Text- und Antwortvorschläge), kostenpflichtige Nutzung ohne Training der Modelle mit den Inhalten. Drittland-Absicherung: EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln.
– Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland (Verarbeitung in den USA, u. a. durch Anthropic, PBC, 548 Market St, PMB 90375, San Francisco, CA 94104, USA) — Claude-API (KI-Auswertung, Assistent „Neo", Text- und Antwortvorschläge, Ergänzung von Produktdaten), kostenpflichtige Nutzung ohne Training der Modelle mit den Inhalten; Ein- und Ausgaben werden beim Anbieter nach 30 Tagen gelöscht. Drittland-Absicherung: EU-Standardvertragsklauseln (Auftragsverarbeitungsvertrag des Anbieters).
– Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA — Versand von E-Mails (Berichte, Hinweise, Bestätigungen). Drittland-Absicherung: EU-US Data Privacy Framework und EU-Standardvertragsklauseln.
– IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland — E-Mail-Postfach für Support-Anfragen.
– Push-Dienste von Apple, Google oder Mozilla — Zustellung von Benachrichtigungen, nur wenn ein Nutzer sie auf seinem Gerät erlaubt; Inhalte ohne Kennzahlen.

AVV als PDF herunterladen (https://good-ads-copilot.de/avv.pdf)

Stand: 20.10.2026