AVV · ART. 28 DSGVO

Auftragsverarbeitungsvertrag

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten gemäß Art. 28 DSGVO zwischen Paldra als Auftragsverarbeiter und dem jeweiligen Kunden als Verantwortlichen.

Parteien

Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) zwischen

AUFTRAGSVERARBEITER

Paldra Technologies
Inhaber: Asmir Kuljancic
Vordere Karlstr. 74
73033 Göppingen
Deutschland
E-Mail: datenschutz@paldra.com
USt-IdNr.: DE458199320

VERANTWORTLICHER

Dem jeweiligen Kunden / Nutzer der Dienste

gemeinsam auch „Parteien“ genannt.

§1 Gegenstand und Dauer der Verarbeitung

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß Art. 28 DSGVO.

Der Auftragsverarbeiter stellt eine Softwareplattform bereit, über die digitale Softwaredienste betrieben werden können, insbesondere:

- KI-gestützte Chatbots
- automatisierte Kommunikationssysteme
- API-basierte Anwendungen
- Analyse- und Automatisierungsfunktionen

Die Verarbeitung erfolgt ausschließlich zur Bereitstellung der vom Verantwortlichen genutzten Dienste.

Die Laufzeit dieses Vertrages richtet sich nach der Dauer der Nutzung der Dienste des Auftragsverarbeiters.

§2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt zu folgenden Zwecken:

- Bereitstellung und Betrieb der Softwareplattform
- Verarbeitung von Nutzeranfragen
- automatisierte Generierung von Antworten durch KI-Systeme
- Kommunikation mit Endnutzern
- Sicherstellung der Systemsicherheit

- Fehleranalyse und Systemverbesserung
- Echtzeit-Anzeige noch nicht abgesendeter Texteingaben von Endnutzern gegenüber Support-Mitarbeitern während eines aktiven Live-Chats (nur temporär, keine dauerhafte Speicherung)

Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen.

Die Dienste dürfen nicht zur Verarbeitung rechtswidriger Inhalte oder zur Verarbeitung personenbezogener Daten verwendet werden, deren Verarbeitung gegen geltendes Datenschutzrecht verstößt.

§ 3 Art der personenbezogenen Daten

Im Rahmen der Nutzung der Dienste können insbesondere folgende Daten verarbeitet werden:

- Name
- E-Mail-Adresse
- Kommunikationsdaten
- Profilangaben aus verbundenen Kanälen (z. B. Benutzername und Profilbild bei Instagram)
- Texteingaben von Nutzern
- Supportanfragen
- Bestelldaten aus verbundenen Shopsystemen (z. B. Bestellnummer, Status, Datum, Artikel, Sendungsnummer, Bezahllink offener Bestellungen)
- Nutzungsdaten
- technische Metadaten (z. B. IP-Adresse, Zeitstempel)

Der Verantwortliche verpflichtet sich, über die Dienste keine besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO (z. B. Gesundheitsdaten, biometrische Daten, politische Meinungen, religiöse Überzeugungen) zu übermitteln, sofern dies nicht ausdrücklich schriftlich vereinbart wurde.

§ 4 Kategorien betroffener Personen

- Besucher von Websites
- Kunden des Verantwortlichen
- Interessenten
- Nutzer digitaler Dienste
- Mitarbeiter des Verantwortlichen

§ 5 Weisungsrecht des Verantwortlichen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich gemäß den dokumentierten Weisungen des Verantwortlichen.

Weisungen können insbesondere erfolgen durch:

- diesen Vertrag
- die Nutzungsbedingungen
- technische Einstellungen innerhalb der Plattform
- schriftliche oder elektronische Anweisungen

Sollte der Auftragsverarbeiter der Auffassung sein, dass eine Weisung gegen geltendes Datenschutzrecht verstößt, informiert er den Verantwortlichen unverzüglich.

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrages sowie gemäß den geltenden datenschutzrechtlichen Vorschriften.

§ 6 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle Personen, die mit der Verarbeitung personenbezogener Daten betraut sind, zur Vertraulichkeit verpflichtet wurden.

Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

§ 7 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter implementiert geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

Hierzu gehören insbesondere:

- Verschlüsselung gespeicherter Zugangsdaten (IMAP-/SMTP-Zugangsdaten und OAuth-Token werden verschlüsselt gespeichert, „at rest“)
- Mandantentrennung: logische Trennung der Daten je Kunde anhand einer eindeutigen Mandantenkennung (shop_id)
- EU-Hosting der Produktivsysteme in Deutschland
- Zugriffskontrolle und Session-Management
- rollenbasierte Zugriffssysteme
- Authentifizierungssysteme
- Mehrfaktor-Authentifizierung für administrative Zugriffe
- verschlüsselte Datenübertragung (TLS-Transportverschlüsselung / HTTPS)
- gesicherte Serverinfrastruktur
- Firewall-Systeme
- Systemüberwachung
- Logging und Monitoring
- regelmäßige, verschlüsselte Backups (off-host innerhalb der EU)
- Wiederherstellungsmechanismen

Die Maßnahmen werden regelmäßig überprüft und bei Bedarf angepasst.

§ 8 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der gesetzlichen Pflichten gemäß DSGVO.

Dies umfasst insbesondere Unterstützung bei:

- der Wahrnehmung von Betroffenenrechten
- Datenschutz-Folgenabschätzungen
- Sicherheitsmaßnahmen
- der Meldung von Datenschutzverletzungen

§ 9 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Datenschutzverletzungen im Zusammenhang mit personenbezogenen Daten.

Die Meldung erfolgt ohne unangemessene Verzögerung und enthält alle relevanten Informationen zur Bewertung des Vorfalls.

§ 10 Unterauftragsverarbeiter (Subprozessoren)

Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter einzusetzen.

Der Auftragsverarbeiter informiert den Verantwortlichen über Änderungen oder Ergänzungen von eingesetzten Unterauftragsverarbeitern in angemessener Form, beispielsweise über die Website oder per elektronischer Mitteilung.

Der Verantwortliche hat das Recht, innerhalb einer angemessenen Frist gegen solche Änderungen Einspruch zu erheben, sofern berechtigte datenschutzrechtliche Gründe vorliegen.

Eine aktuelle Liste der eingesetzten Unterauftragsverarbeiter ist jederzeit auf der Website des Auftragsverarbeiters unter https://paldra.com/subprocessors abrufbar.

Zu den möglichen Unterauftragsverarbeitern gehören insbesondere:

ANBIETER	ZWECK	STANDORT	GRUNDLAGE
Immer im Einsatz			
Hetzner Online GmbH Datenschutzhinweise	Hosting / Speicherung / Backup (Cloud-Infrastruktur)	Deutschland (EU)	EU
Anthropic, PBC Datenschutzhinweise	KI / Sprachmodell (LLM) für Antworten, automatische Prüfung, Bildbeschreibung und Auswertungen (Claude)	USA	SCC · DPF
OpenAI Datenschutzhinweise	KI / Sprachmodell (LLM) als Ersatz und zur Lastverteilung	USA	SCC · DPF
Mistral AI Datenschutzhinweise	KI / Sprachmodell (LLM), Embeddings, OCR, Transkription	Frankreich (EU)	EU
Microsoft Ireland Operations Ltd. / Microsoft Corp. Datenschutzhinweise	E-Mail-Versand (Microsoft Graph) sowie optional angebundenes Outlook-Postfach	Irland (EU) / USA	SCC · DPF
Stripe, Inc. Datenschutzhinweise	Zahlungsabwicklung	USA	SCC · DPF
Cloudflare, Inc. Datenschutzhinweise	DNS / CDN / Proxy	USA	SCC · DPF

Nur wenn der Verantwortliche die Funktion nutzt			
Google LLC Datenschutzhinweise	Optional angebundenes Gmail-Postfach; Anmeldung am Konto („Mit Google anmelden“); Zustellung von Push-Benachrichtigungen an Android-/Chrome-Geräte	USA	SCC · DPF
Apple Inc. Datenschutzhinweise	Anmeldung am Konto („Mit Apple anmelden“); Zustellung von Push-Benachrichtigungen an Safari-/iOS-Geräte	USA	SCC · DPF
Meta Platforms Ireland Ltd. / Meta Platforms, Inc. Datenschutzhinweise	Optional angebundene Kanäle Instagram / WhatsApp	Irland (EU) / USA	SCC · DPF
Shopify International Ltd. Datenschutzhinweise	Vom Händler aktivierte Integration: Produkt-, Bestell-, Kunden-, Retourendaten und Rechtstexte des Shops; App-Abrechnung über Shopify	Irland (EU) / Kanada, USA	SCC · DPF

EU = Verarbeitung in der EU. SCC · DPF = EU-Standardvertragsklauseln und, soweit der Anbieter zertifiziert ist, EU-US Data Privacy Framework (Art. 44 ff. DSGVO).

Der Auftragsverarbeiter stellt sicher, dass alle eingesetzten Unterauftragsverarbeiter vertraglich zur Einhaltung der datenschutzrechtlichen Anforderungen gemäß Art. 28 DSGVO verpflichtet werden.

§ 11 Internationale Datenübermittlung

Eine Übermittlung personenbezogener Daten in Staaten außerhalb des Europäischen Wirtschaftsraums kann erfolgen.

Eine solche Übermittlung erfolgt ausschließlich unter Einhaltung der gesetzlichen Anforderungen gemäß Art. 44 ff. DSGVO.

Hierzu können insbesondere folgende Mechanismen eingesetzt werden:

- EU-Standardvertragsklauseln (SCC)
- EU-US Data Privacy Framework (DPF), soweit der jeweilige US-Unterauftragsverarbeiter zertifiziert ist
- Angemessenheitsbeschlüsse der Europäischen Kommission
- oder vergleichbare gesetzliche Garantien gemäß DSGVO, soweit dies für die Bereitstellung der Dienste erforderlich ist

Für US-Unterauftragsverarbeiter (insbesondere Microsoft Corp., Google LLC, Apple Inc., Meta Platforms, Inc., Stripe, Inc. und Cloudflare, Inc.) erfolgt die Übermittlung auf Grundlage der EU-Standardvertragsklauseln und – soweit das jeweilige Unternehmen zertifiziert ist – des EU-US Data Privacy Frameworks gemäß Art. 44 ff. DSGVO.

Für die KI-Unterauftragsverarbeiter Anthropic, PBC und OpenAI (USA) erfolgt die Übermittlung auf Grundlage der EU-Standardvertragsklauseln (jeweiliges Data Processing Addendum) gemäß Art. 46 DSGVO.

§ 12 Löschung und Rückgabe von Daten

Nach Beendigung des Vertrags bzw. der Nutzung der Dienste werden die personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. g DSGVO nach Wahl des Verantwortlichen gelöscht oder zurückgegeben, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

Chat- und Konversationsdaten werden regulär für die Dauer von 12 Monaten aufbewahrt und anschließend gelöscht.

Backups werden im Rahmen der üblichen Sicherungszyklen gelöscht.

§13 Kontrollrechte

Der Verantwortliche ist berechtigt, die Einhaltung dieses Vertrages zu überprüfen.

Der Auftragsverarbeiter stellt dem Verantwortlichen alle notwendigen Informationen zur Verfügung, um die Einhaltung der DSGVO nachweisen zu können.

Solche Überprüfungen dürfen den Geschäftsbetrieb des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigen und sind mit angemessener Vorankündigung durchzuführen.

Die Kosten eines Audits trägt grundsätzlich der Verantwortliche, sofern nicht ein erheblicher Verstoß gegen datenschutzrechtliche Bestimmungen durch den Auftragsverarbeiter festgestellt wird.

§14 Haftung

Soweit gesetzlich zulässig, ist die Haftung des Auftragsverarbeiters für Schäden aus oder im Zusammenhang mit diesem Vertrag auf den Betrag begrenzt, den der Verantwortliche in den zwölf (12) Monaten vor Eintritt des schadensbegründenden Ereignisses an den Auftragsverarbeiter gezahlt hat.

Diese Haftungsbegrenzung gilt nicht bei:

- Vorsatz
- grober Fahrlässigkeit
- Verletzung von Leben, Körper oder Gesundheit
- zwingenden gesetzlichen Haftungsvorschriften

§15 Schlussbestimmungen

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Es gilt das Recht der Bundesrepublik Deutschland.

Gerichtsstand ist – soweit gesetzlich zulässig – der Sitz des Auftragsverarbeiters.

§16 Nutzung von KI-Systemen

Der Auftragsverarbeiter kann zur Bereitstellung der Dienste automatisierte Systeme einschließlich künstlicher Intelligenz einsetzen.

Dabei werden die vom Verantwortlichen übermittelten Daten ausschließlich zur Generierung von Antworten und zur Bereitstellung der Dienste verarbeitet.

Die Daten werden nicht zum Training von KI-Modellen verwendet, weder durch den Auftragsverarbeiter noch durch dessen Unterauftragsverarbeiter.

Davon zu unterscheiden ist das Lernen aus Fällen: Der Auftragsverarbeiter kann aus bereits beantworteten Anfragen Beispiele (Frage und Antwort) ableiten und in der Wissensbasis des Verantwortlichen speichern, um künftige Antworten für den Verantwortlichen zu verbessern. Dabei wird kein KI-Modell trainiert oder verändert. Diese Beispiele werden ausschließlich für den Verantwortlichen verwendet, nicht an Dritte weitergegeben und mit dessen Daten gelöscht. Der Verantwortliche kann diese Funktion jederzeit in seinem Dashboard deaktivieren.

Ebenso kann der Auftragsverarbeiter aus Anfragen, die Mitarbeiter des Verantwortlichen abgeschlossen haben, Abläufe ableiten (Art des Anliegens, vom Kunden benötigte Angaben, Schritte des Teams, Ergebnis) und in der Wissensbasis des Verantwortlichen speichern („Gelernte Abläufe"). Erkennbare personenbezogene Daten werden vor der Verarbeitung durch KI-Systeme und vor dem Speichern entfernt; gespeichert werden der Ablauf ohne Bezug zu einzelnen Kunden, die Zahl der Fälle, die beteiligten Teammitglieder und je Fall ein nicht umkehrbarer Schlüssel, der mit dem Gespräch gelöscht wird. Dabei wird kein KI-Modell trainiert oder verändert. Fälle mit besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) und Daten aus der Gmail-API werden nicht verwendet; es wird nur aus Gesprächen gelernt, die nach dem Einschalten der Funktion begonnen haben. Der Verantwortliche kann die Funktion je Kanal deaktivieren und jeden Ablauf einsehen, ändern, pausieren und löschen. Ordnet das System einen Ablauf als Regel ein, die das Team immer oder unter einer bestimmten Bedingung so handhabt, darf der KI-Assistent dessen Schritte und Ergebnis nennen, solange der Verantwortliche das Lernen eingeschaltet hat; ohne Durchsicht durch das Team nur, wenn der Ablauf mindestens dreimal vorkam und der Wissensbasis nicht widerspricht. Andere Abläufe nennt er nur mit Erlaubnis des Verantwortlichen. Die vom Team genannte Rücksendeadresse des Verantwortlichen kann beim Ablauf gespeichert werden. Ein Ablauf, der zwölf Monate nicht wieder vorkam, wird gelöscht.

Hat der Verantwortliche ein Outlook- oder IMAP-Postfach verbunden und ist das Lernen aus E-Mails eingeschaltet, wertet der Auftragsverarbeiter dafür auch Antworten aus, die Mitarbeiter des Verantwortlichen direkt in diesem Postfach gesendet haben (Ordner der gesendeten Elemente), nach denselben Regeln und nur ab dem Einschalten; Postfächer, die über die Gmail-Schnittstelle von Google verbunden sind, sind ausgenommen. Ändern Mitarbeiter einen KI-Entwurf vor dem Senden, zählt der Auftragsverarbeiter je Verantwortlichem ohne Text, welche Art von Angebot gestrichen oder belassen wurde, und schlägt wiederholt gestrichene Angebote nicht mehr von sich aus vor; Hinweise auf gesetzliche Rechte der Kunden werden dadurch nie unterdrückt. Diese Zählungen werden nach zwölf Monaten gelöscht.

Auf ausdrückliche Anfrage eines Kunden des Verantwortlichen kann der Auftragsverarbeiter genau ein angefragtes Dokument je Antwort übermitteln: Dateien, die der Verantwortliche in seiner Wissensbasis dafür freigegeben hat, öffentlich auf dessen Website abrufbare PDF-Dateien sowie – nach Prüfung der Identität wie bei der Rechnungsauskunft – Rechnungen als PDF aus den vom Verantwortlichen verbundenen Rechnungsdiensten. Nicht freigegebene Dateien der Wissensbasis werden nicht an Kunden übermittelt. Jede übermittelte Datei wird an der Nachricht im Gesprächsverlauf gespeichert und mit dem Gespräch gelöscht.

Die durch KI-Systeme generierten Inhalte erfolgen automatisiert auf Grundlage der vom Verantwortlichen oder dessen Nutzern übermittelten Eingaben.

Der Auftragsverarbeiter übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit oder rechtliche Zulässigkeit der durch KI-Systeme generierten Inhalte.

Der Verantwortliche ist dafür verantwortlich, die Ergebnisse der Systeme zu überprüfen und deren Nutzung im Einklang mit geltendem Recht sicherzustellen.

§ 17 Inkrafttreten

Dieser Auftragsverarbeitungsvertrag tritt automatisch mit der Nutzung der Dienste des Auftragsverarbeiters oder dem Abschluss eines entsprechenden Hauptvertrages zwischen den Parteien in Kraft.