Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO - Version 1.3 - Erstellt am 09.09.2026

Vertragsparteien

Verantwortlicher (nachfolgend „Auftraggeber")

Unternehmen	[Ihr Unternehmensname]
Ansprechpartner	[Ihr Ansprechpartner]
Anschrift	[Ihre Anschrift]
E-Mail	[ihre-mail@example.de]

Auftragsverarbeiter (nachfolgend „Auftragnehmer")

Unternehmen	Marcus Euchner - Platrion
Anschrift	Lange Gasse 34, 72581 Dettingen an der Erms, Deutschland
E-Mail	info@platrion.de
Telefon	+49 157 73551423

1. Gegenstand und Dauer der Verarbeitung

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der im Hauptvertrag (Projekt- bzw. Servicevertrag) vereinbarten Leistungen. Soweit nicht abweichend vereinbart, umfasst dies insbesondere:

• Individuelle Enterprise-Plattform mit Multi-Mandantenfähigkeit, vollständigem Compliance-Paket (DSGVO, GoBD, eIDAS), Key-Rotation, Disaster-Recovery-Plan sowie dedizierter Support. Agentengestützte Features (Text-/Bild-Auswertung) bei aktiver Buchung. Monatlicher Full-Managed-Service. Hosting inklusive.

(2) Dauer: Für die Dauer des Hauptvertrags (Projekt- bzw. Servicevertrag).

(3) Die Verarbeitung erfolgt ausschließlich im Gebiet der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Eine Übermittlung in Drittländer erfolgt nur, wenn die besonderen Voraussetzungen von Art. 44 ff. DSGVO erfüllt sind.

2. Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag und umfassen insbesondere:

• Hosting und technischer Betrieb der Website / Plattform
• Wartung, Updates und Fehlerbehebung
• Regelmäßige Backups, Disaster-Recovery und Verfügbarkeitsmonitoring
• Bearbeitung von Kontaktformular- und Anfrage-Eingaben
• Bereitstellung eines Admin-Panels für den Auftraggeber
• Erstellung von Angeboten, Rechnungen und Zahlungsabwicklung
• Datenschutzkonforme Traffic-Analyse (keine Third-Party-Cookies)
• Rechtssichere digitale Signaturen inkl. Audit-Trail (eIDAS)
• Verwaltung mehrerer Mandanten / Nutzergruppen und rollenbasierte Zugriffe
• KI-gestützte Text- oder Bildverarbeitung (nur bei aktiv gebuchten Features)

3. Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten werden verarbeitet:

• IP-Adressen und technische Metadaten (Zugriffslogs, User-Agent)
• Inhaltsdaten aus Kontaktformularen (Name, E-Mail, Telefon, Freitextnachricht)
• Stammdaten (Name, Firma, Anschrift des Auftraggebers)

• Vertrags- und Abrechnungsdaten (Rechnungen, Angebote, Zahlungsstatus)
• Login- und Nutzungsdaten der Plattform (E-Mail, Login-Zeitpunkte, IP, Session-IDs)
• Zahlungs-Metadaten (Kartenmaske, Transaktions-ID) - die eigentliche Kartendaten-Verarbeitung erfolgt PCI-DSS-konform beim Payment-Provider
• Vom Auftraggeber eingestellte Inhalte (Texte, Bilder, Dokumente)
• KI-Prompts und -Antworten (nur bei aktiv gebuchten KI-Features; keine Nutzung für Modelltraining laut Vertrag mit KI-Anbieter)

4. Kategorien betroffener Personen

• Beschäftigte des Verantwortlichen (Auftraggeber)
• Kunden und Interessenten des Verantwortlichen
• Besucher der Website bzw. Plattform
• Lieferanten und Geschäftspartner

5. Pflichten des Auftragnehmers

(1) Verarbeitung der Daten ausschließlich im Rahmen der dokumentierten Weisungen des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO). Mündliche Weisungen werden unverzüglich schriftlich bestätigt.

(2) Sicherstellung, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(3) Umsetzung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO (siehe Anlage 1 - TOM).

(4) Unterstützung des Auftraggebers bei der Erfüllung der Betroffenenrechte (Art. 12-22 DSGVO) durch geeignete technische und organisatorische Maßnahmen.

(5) Unterstützung des Auftraggebers bei Datenschutz-Folgenabschätzungen (Art. 35, 36 DSGVO) und bei der Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO).

(6) Nach Abschluss der Erbringung der Verarbeitungsleistungen, nach Wahl des Auftraggebers Löschung oder Rückgabe aller personenbezogenen Daten sowie Löschung vorhandener Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g DSGVO).

(7) Benennung eines Ansprechpartners für Datenschutzfragen beim Auftragnehmer: Marcus Ehrenhofer, info@platrion.de.

(8) Führung eines Verzeichnisses aller Verarbeitungstätigkeiten im Auftrag des Auftraggebers nach Art. 30 Abs. 2 DSGVO.

(9) Bereitstellung aller erforderlichen Informationen zum Nachweis der Einhaltung dieser Verpflichtungen (Art. 28 Abs. 3 lit. h DSGVO) sowie Ermöglichung und Unterstützung von Audits durch den Auftraggeber oder einen von ihm beauftragten Prüfer (mit angemessener Vorankündigung, werktags).

(10) Unverzügliche Information des Auftraggebers, wenn nach Ansicht des Auftragnehmers eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt.

6. Unterauftragsverhältnisse (Subunternehmer)

(1) Der Auftraggeber erteilt hiermit die allgemeine schriftliche Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Subunternehmer) gemäß Art. 28 Abs. 2 DSGVO.

(2) Der Auftragnehmer setzt derzeit folgende Subunternehmer ein:

• Hosting-Provider (Rechenzentrum in Deutschland, ausschließlich EU/EWR) - Server-Infrastruktur, DDoS-Schutz, TLS-Terminierung
• Resend, Inc. (via EU-Endpoint) - transaktionaler E-Mail-Versand (Kontaktformulare, Bestätigungen, System-Mails); Datenübermittlung in die USA nach EU-U.S. Data Privacy Framework (Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023)
• Stripe Payments Europe Ltd., Dublin, Irland - Kartenzahlung, Apple Pay, Google Pay (nur bei aktivem Payment-Modul im gebuchten Paket)
• PayPal (Europe) S.à r.l. et Cie, S.C.A., Luxemburg - Zahlungsabwicklung PayPal (nur bei aktivem PayPal-Modul im gebuchten Paket)
• OpenAI Ireland Ltd., Dublin, Irland - optionale KI-Text- und Bilderzeugung; nur bei explizit gebuchten KI-Features aktiviert, keine Endkundendaten übermittelt
• Anthropic PBC, San Francisco, USA - optionale KI-Textverarbeitung (Claude); nur bei explizit gebuchten

KI-Features aktiviert; DPF-Zertifizierung
• Google Ireland Ltd. (Gemini API) - optionale Bild-/Text-KI-Verarbeitung; nur bei explizit gebuchten KI-Features aktiviert
(3) Mit sämtlichen Subunternehmern, die personenbezogene Daten verarbeiten, bestehen entsprechende Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO bzw. Standardvertragsklauseln, soweit eine Übermittlung in Drittländer erfolgt.
(4) Der Auftragnehmer informiert den Auftraggeber rechtzeitig vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder den Austausch weiterer Auftragsverarbeiter. Der Auftraggeber kann der Änderung binnen 30 Tagen aus wichtigem Grund widersprechen.

7. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragnehmer hat die in Anlage 1 näher beschriebenen technischen und organisatorischen Maßnahmen getroffen und hält diese während der Vertragslaufzeit auf einem dem Stand der Technik entsprechenden Niveau.

8. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne der DSGVO Verantwortlicher für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung insgesamt.
(2) Der Auftraggeber hat das Recht, sich jederzeit von der Einhaltung der getroffenen Maßnahmen zu überzeugen. Der Auftragnehmer wird nach vorheriger Terminabstimmung Einsicht in Dokumentationen und relevante Systeme gewähren. Umfangreiche Prüfungen werden nach Aufwand abgerechnet, soweit sie über eine jährliche Auskunft hinausgehen.

9. Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer meldet dem Auftraggeber jede ihm bekanntgewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntnisnahme. Die Meldung enthält mindestens die in Art. 33 Abs. 3 DSGVO genannten Informationen.
(2) Der Auftraggeber bleibt für die Erfüllung seiner Meldepflicht gegenüber der Aufsichtsbehörde (72-Stunden-Frist) verantwortlich.

10. Rückgabe und Löschung von Daten

(1) Mit Beendigung der Leistungserbringung wird der Auftragnehmer auf Wahl des Auftraggebers die Daten entweder vollständig zurückgeben (z. B. als JSON/XLSX-Export) oder datenschutzkonform löschen.
(2) Die Löschung wird schriftlich bestätigt. Gesetzliche Aufbewahrungspflichten (insbesondere handels- und steuerrechtliche) bleiben unberührt; entsprechende Daten werden bis zum Ablauf der jeweiligen Fristen mit Zugriffsbeschränkung aufbewahrt.

11. Haftung

Die Haftung richtet sich nach den Regelungen des Hauptvertrags. Für Ansprüche Betroffener nach Art. 82 DSGVO gelten die dort getroffenen Bestimmungen.

12. Schlussbestimmungen

(1) Es gilt ausschließlich deutsches Recht. Gerichtsstand ist Reutlingen.
(2) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
(3) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Änderung dieses Schriftformerfordernisses.
(4) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV vor, soweit datenschutzrechtliche Belange betroffen sind.

Unterschriften

Ort, Datum, Unterschrift Auftraggeber ([Ihr Unternehmensname])	Dettingen an der Erms, 09.09.2026 - Marcus Euchner Auftragnehmer (Marcus Euchner, Platrion)

Anlage 1 - Technische und organisatorische Maßnahmen

gemäß Art. 32 DSGVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Zutrittskontrolle: Die Verarbeitung erfolgt ausschließlich in gesicherten Rechenzentren der Hosting-Provider mit kontrolliertem Zutritt, Videoüberwachung und Alarmanlagen.
• Zugangskontrolle: Zugriff auf Systeme ausschließlich per individuellem Login, starke Passwortrichtlinie, 2-Faktor-Authentifizierung für administrative Zugänge.
• Zugriffskontrolle: Rollen- und berechtigungsbasiertes Konzept, Minimalprinzip. Mandantenfähige Trennung auf Datenbankebene.
• Trennungskontrolle: Logische Trennung der Kundendaten pro Mandant. Produktions- und Entwicklungsumgebungen sind getrennt.
• Pseudonymisierung, soweit möglich; Verschlüsselung sensibler Felder.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

• Weitergabekontrolle: Datenübertragung ausschließlich verschlüsselt (TLS 1.2+).
• Eingabekontrolle: Protokollierung administrativer Änderungen im System-Log.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Verfügbarkeitskontrolle: Redundante Infrastruktur, automatische Failover bei kritischen Komponenten, regelmäßige Sicherheitsupdates.
• Backup-Konzept: Tägliche automatische Backups der Datenbank, wöchentliche vollständige Backups, Aufbewahrung mindestens 7 Tage.
• Notfallplan: Dokumentierter Disaster-Recovery-Plan mit definierten Wiederherstellungszeiten.

Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

• Datenschutz-Management: Regelmäßige Selbstprüfung und Dokumentation im Verarbeitungsverzeichnis.
• Incident-Response-Management: Definierte Abläufe zur Meldung und Behandlung von Sicherheitsvorfällen innerhalb von 24 Stunden.
• Datenschutzfreundliche Voreinstellungen (Privacy by Default / by Design) gemäß Art. 25 DSGVO.
• Auftragskontrolle: Vertragliche Bindung aller Unterauftragsverarbeiter nach Art. 28 DSGVO.

Die vorgenannten Maßnahmen werden regelmäßig überprüft und dem Stand der Technik angepasst. Wesentliche Änderungen werden dem Auftraggeber in geeigneter Form mitgeteilt.