

Auftragsverarbeitungsvertrag (AVV)

Contents

Auftragsverarbeitungsvertrag (AVV)	1
Präambel	1
§ 1 — Gegenstand und Dauer der Verarbeitung	2
§ 2 — Art und Zweck der Verarbeitung	2
§ 3 — Pflichten des Auftragnehmers	3
§ 4 — Rechte und Pflichten des Auftraggebers	4
§ 5 — Meldung von Datenschutzverletzungen	5
§ 6 — Datentransfer in Drittländer	5
§ 7 — Haftung	6
§ 8 — Vertragslaufzeit und Kündigung	6
§ 9 — Form, Änderungen, Sprache	6
§ 10 — Anwendbares Recht und Gerichtsstand	7
§ 11 — Anlage A: Technische und organisatorische Maßnahmen (TOMs)	7
§ 12 — Anlage B: Sub-Auftragsverarbeiter	9
Akzeptanz-Hinweis	10

Auftragsverarbeitungsvertrag (AVV)

Version: 2026-08 **Gültig ab:** 2026-07-24 **Sprache:** Deutsch (verbindlich) **Vorgänger:** [avv-2026-07.md](#) **Änderung gegenüber 2026-07 (Hosting-Umzug weg von Hostinger):** Infrastruktur-Angaben (§ 6) und Sub-Auftragsverarbeiter-Liste (Anlage B) sowie Anlage A (TOMs) aktualisiert. Kiosk-Update-Hosting [updates.boothpilot.app](#) von Hostinger → **BunnyWay d.o.o. (Bunny.net)**; E-Mail-Postfach hallo@boothpilot.de + DNS-Zone boothpilot.de von Hostinger → **ALL-INKL.COM – Neue Medien Münnich**. **Hostinger entfällt als Sub-Auftragsverarbeiter** (nur noch Domain-Registrar — keine Verarbeitung personenbezogener Daten im Auftrag). Beide neuen Anbieter mit Sitz in der EU (Slowenien bzw. Deutschland), kein Drittlandtransfer; AVV/DPA mit beiden abgeschlossen. Keine Änderung an den Vertragsklauseln §§ 1–10.

Präambel

Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten zwischen dem Verantwortlichen (im Folgenden „Auftraggeber“) und dem Auftragsverarbeiter (im Folgenden „Auftragnehmer“) gemäß **Art. 28 DSGVO**.

Auftraggeber: Der Operator (Inhaber eines BoothPilot-Accounts), der die Software für die Bereitstellung von Foto-Box-Dienstleistungen einsetzt. Persönliche Daten des Auftraggebers werden bei Account-Anlage erfasst.

Auftragnehmer:



Bastian Egelseer (BoothPilot.de) Altmannshof 15 92284 Poppenricht Deutschland E-Mail: hallo@boothpilot.de

Mit Akzeptanz dieser Vereinbarung im Onboarding-Wizard auf boothpilot.app/dashboard/onboarding/avv bestätigt der Auftraggeber den Vertragsschluss. Die Akzeptanz wird mit Zeitstempel, Vertragsversion, IP-Adresse und User-Agent in der Datenbank des Auftragnehmers protokolliert (Tabelle `avv_acceptances`, siehe § 9).

§ 1 — Gegenstand und Dauer der Verarbeitung

1.1 Gegenstand

Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers personenbezogene Daten zum Zweck der Bereitstellung der BoothPilot-Plattform. Die Plattform umfasst:

- **Foto-Box-Software** (Kiosk-App auf Operator-Hardware)
- **Online-Galerie** für Veranstaltungs-Fotos (`boothpilot.app/g/[slug]`)
- **Buchungs-Magic-Link-Portal** für Endkunden (`boothpilot.app/buchung/[token]`)
- **Operator-Dashboard** zur Verwaltung von Buchungen, Boxen, Galerien und Templates
- **Operator-Website** auf Subdomain oder Custom-Domain (`<name>.boothpilot.app` bzw. eigene Domain via CNAME)
- **Zahlungs-Vermittlung** für Endkunden-Buchungen (PayPal-Order-Erstellung, PDF-Rechnungs-Generierung für Banküberweisung — der Auftragnehmer ist **nicht** Treuhänder, Geld fließt direkt zwischen Endkunde und Auftraggeber)

1.2 Dauer

Die Verarbeitung beginnt mit Account-Aktivierung des Auftraggebers (Beta-Aktivierung, Self-Service-Trial-Start, oder Plan-Konvertierung über Stripe-Subscription) und endet mit Vertragsbeendigung oder Account-Löschung.

§ 2 — Art und Zweck der Verarbeitung

2.1 Datenkategorien

Der Auftragnehmer verarbeitet im Auftrag folgende Kategorien personenbezogener Daten:

Kategorie	Konkrete Daten	Quelle
Operator-Stammdaten	Name, E-Mail, Geschäftsanschrift, Steuer-/USt-IdNr., Bankverbindung (IBAN/BIC), PayPal-Email für Zahlungs-Empfang, Branding-Konfiguration, Subdomain, Plan, Stripe-Customer-/Subscription-IDs	Account-Anlage durch Auftraggeber



Kategorie	Konkrete Daten	Quelle
Endkunden-Daten (Buchungen)	Name, E-Mail, Telefon, Event-Datum, Veranstaltungs-Adresse, Magic-Link-Token, Rechnungs-Anschrift (für Firmenkunden mit Banküberweisung)	Buchungsformular auf Auftraggeber-Website
Zahlungs-Metadaten	PayPal-Order-IDs, PayPal-Bestätigungs-Zeitstempel, Rechnungsnummern, Zahlungsstatus	PayPal-Webhook, Operator-manuelle Markierung
Foto-Daten (Gäste-Fotos)	JPEG-Bilder mit Personenabbildungen	Foto-Box-Aufnahmen während Veranstaltungen
Galerie-Metadaten	Galerie-Slug, PIN, Ablaufdatum, Druck-Limits, DSGVO-Consent-Flag	Auftraggeber-Konfiguration je Event
Druck-Logs	Foto-Referenz, Anzahl Drucke, Zeitstempel	Foto-Box-Bridge-Server
Audit-Logs	Aktor-Typ + ID, Aktion, Zeitstempel, IP-Adresse, User-Agent	Automatisch bei jeder fachlichen Aktion (DSGVO-Nachweispflicht)
Box-Telemetrie	Hardware-ID, Heartbeat-Timestamps, Versions-Strings, Drucker-/Kamera-Status	Foto-Box automatisch (alle 600 s)

2.2 Betroffene Personen

Kategorie	Beispiele
Endkunden des Auftraggebers	Brautpaare, Veranstalter, Geschäftskunden, die Foto-Boxen buchen
Veranstaltungsgäste	Personen, die an einer Foto-Box-Veranstaltung teilnehmen und fotografiert werden
Auftraggeber selbst	Inhaber des BoothPilot-Accounts mit personenbezogenen Stammdaten

2.3 Zweckbindung

Der Auftragnehmer verarbeitet die Daten **ausschließlich** zum Zweck der Vertragserfüllung gemäß § 1.1. Eine Verarbeitung für eigene Zwecke (z.B. Werbung, Profiling, Verkauf an Dritte) findet **nicht** statt. Aggregierte, nicht-personenbezogene Statistiken zur Plattform-Verbesserung sind ausgenommen.

§ 3 — Pflichten des Auftragnehmers

3.1 Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisungen des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO). Die Vertragserfüllung selbst stellt eine fortlaufende Weisung dar; ergänzende Weisungen können in Textform (z.B. E-Mail an hallo@boothpilot.de) erteilt werden.



3.2 Vertraulichkeit

Der Auftragnehmer verpflichtet alle Personen, die Zugang zu personenbezogenen Daten haben, schriftlich zur Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO). Aktuell besteht der Mitarbeiterkreis aus dem Inhaber selbst (Bastian Egelseer); jeder zukünftige Mitarbeiter wird vor Aufgabenaufnahme vertraulich verpflichtet.

3.3 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragnehmer ergreift die in Anlage A (§ 11) beschriebenen Maßnahmen nach Art. 32 DSGVO und überprüft sie regelmäßig.

3.4 Sub-Auftragsverarbeiter

Eine Übersicht aller eingesetzten Sub-Auftragsverarbeiter findet sich in Anlage B (§ 12). Der Auftragnehmer informiert den Auftraggeber **mindestens 30 Tage vor** jeder geplanten Änderung (Hinzufügung, Austausch). Der Auftraggeber kann Änderungen aus wichtigem Grund widersprechen; in diesem Fall können beide Parteien das Vertragsverhältnis ordentlich kündigen.

3.5 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber bei:

- **Betroffenenrechten** (Art. 12–23 DSGVO): Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch — über das Operator-Dashboard und auf direkte Anfrage
- **Datenschutz-Folgenabschätzungen** (Art. 35 DSGVO): Bereitstellung notwendiger Informationen zur eigenen Verarbeitung
- **Meldungen von Datenschutzverletzungen** (Art. 33–34 DSGVO): unverzügliche Information über Vorfälle, betroffene Datenkategorien, geschätzte Anzahl betroffener Personen, geplante Maßnahmen — siehe § 5

3.6 Löschung und Rückgabe nach Vertragsende

Nach Beendigung des Vertrags löscht der Auftragnehmer alle personenbezogenen Daten innerhalb von **30 Tagen**, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen (insb. Rechnungen nach § 257 HGB / § 147 AO: 10 Jahre Aufbewahrungspflicht). Eine Rückgabe in maschinenlesbarem Format (JSON-Export) ist auf Anfrage möglich. Backups werden nach Ablauf der Backup-Rotation (max. 90 Tage) automatisch überschrieben.

3.7 Nachweispflicht

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die zur Erfüllung der Auskunftspflichten notwendigen Informationen zur Verfügung, insbesondere TOM-Beschreibung und Sub-Verarbeiter-Übersicht.

§ 4 — Rechte und Pflichten des Auftraggebers

4.1 Verantwortlichkeit

Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO. Er entscheidet über Zwecke und Mittel der Verarbeitung der von ihm erhobenen Daten und ist gegenüber den betroffenen Personen primär auskunfts- und meldepflichtig.



4.2 Pflichtaushänge auf Veranstaltungen

Der Auftraggeber stellt sicher, dass auf Veranstaltungen, bei denen die Foto-Box eingesetzt wird, ein DSGVO-konformer Aushang sichtbar ist (Art. 13 DSGVO Informationspflicht). Eine Vorlage bietet BoothPilot im Operator-Dashboard zum Download an.

4.3 Endkunden-Information

Der Auftraggeber informiert seine Endkunden (Buchungskunden) auf seiner Website über Datenverarbeitung durch BoothPilot als Auftragsverarbeiter, einschließlich Hinweis auf PayPal als Zahlungs-Sub-Auftragsverarbeiter (sofern relevant). Eine Datenschutz-Erklärungs-Vorlage stellt der Auftragnehmer im Operator-Dashboard bereit.

4.4 Weisungsbefugnis

Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung in Textform zu erteilen, soweit diese nicht der Funktionsweise der Plattform widersprechen. Mündliche Weisungen sind unverzüglich zu bestätigen.

4.5 Kontrollrecht

Der Auftraggeber hat das Recht, sich von der Einhaltung der Datenschutzpflichten beim Auftragnehmer zu überzeugen — durch Einsichtnahme in Dokumentation oder durch zertifizierte externe Prüfer auf eigene Kosten. Anfragen sind mit angemessener Frist (≥14 Tage) zu stellen.

§ 5 — Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten (Datenpanne) **unverzüglich, spätestens innerhalb von 24 Stunden** nach Kenntnisnahme. Die Meldung enthält:

- Beschreibung der Art der Verletzung
- Betroffene Datenkategorien und Anzahl betroffener Personen (geschätzt)
- Wahrscheinliche Folgen
- Bereits ergriffene oder geplante Gegenmaßnahmen
- Kontakt für Rückfragen

Die Meldung erfolgt an die im Operator-Dashboard hinterlegte Operator-E-Mail-Adresse. Der Auftraggeber ist seinerseits zur Meldung an die Aufsichtsbehörde verpflichtet (Art. 33 DSGVO, 72 Std.) und ggf. an betroffene Personen (Art. 34 DSGVO).

§ 6 — Datentransfer in Drittländer

Der Auftragnehmer betreibt seine Infrastruktur primär in der **Europäischen Union**:

- **Datenbank + Storage:** Supabase (eu-central-1, Frankfurt)
- **Web-Hosting:** Vercel (fra1-Region, Frankfurt)
- **Update-Hosting (Kiosk-Bundles):** BunnyWay d.o.o. / Bunny.net (Storage-Region Falkenstein, Deutschland)



- **E-Mail-Postfach + DNS (boothpilot.de):** ALL-INKL.COM – Neue Medien Münnich (Friedersdorf, Deutschland)
- **Cron-Scheduling:** Upstash QStash (eu-west-1, Frankfurt)
- **E-Mail-Versand:** Resend (EU-Region)

Sub-Auftragsverarbeiter mit Sitz außerhalb der EU sind in Anlage B aufgeführt. Soweit Datenübermittlungen an Drittländer erforderlich sind, erfolgen sie ausschließlich auf Basis eines Angemessenheitsbeschlusses der EU-Kommission (insb. EU-US Data Privacy Framework) oder Standardvertragsklauseln (SCCs).

§ 7 — Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für die ihr zuzurechnenden Datenschutzverstöße. Der Auftragnehmer haftet nicht für Datenschutzverstöße, die auf einer Weisung des Auftraggebers beruhen, soweit diese Weisung erkennbar nicht offensichtlich rechtswidrig war.

§ 8 — Vertragslaufzeit und Kündigung

8.1 Laufzeit

Dieser Vertrag tritt mit Akzeptanz im Onboarding-Wizard in Kraft und gilt für die gesamte Vertragsdauer der zugrunde liegenden Software-Nutzung (Beta-Phase, Self-Service-Trial oder Subscription).

8.2 Kündigung

Mit Beendigung des Hauptvertrages (Account-Löschung, Subscription-Kündigung, Beta-Ablauf ohne Verlängerung) endet auch dieser AVV. Eine separate Kündigung dieses AVV ist nicht möglich, solange der Hauptvertrag besteht.

8.3 Pflichten nach Vertragsende

Nach Vertragsende gelten die Lösch- und Rückgabepflichten gemäß § 3.6.

§ 9 — Form, Änderungen, Sprache

9.1 Akzeptanz

Die Akzeptanz erfolgt elektronisch im Onboarding-Wizard. Die akzeptierte Version, der Zeitpunkt, die IP-Adresse und der User-Agent werden in der Tabelle `avv_acceptances` dauerhaft gespeichert (DSGVO-konform pseudonymisiert).

9.2 Änderungen

Änderungen werden als neue Version (z.B. `avv-2026-06.md`) veröffentlicht. Bestehende Auftraggeber werden bei nächster Anmeldung im Dashboard zur erneuten Akzeptanz aufgefordert. Bis zur erneuten Akzeptanz bleibt die letzte vom Auftraggeber akzeptierte Version verbindlich.



9.3 Vertragssprache

Verbindlich ist die deutsche Fassung. Englische Übersetzungen werden ggf. zur Verfügung gestellt, sind aber nicht verbindend.

9.4 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Anstelle der unwirksamen Bestimmung gilt die gesetzliche Regelung.

9.5 Rangfolge

Bei Widersprüchen zwischen diesem AVV und sonstigen Vertragsbestandteilen (AGB, Hauptvertrag) gelten die Bestimmungen dieses AVV vorrangig.

§ 10 — Anwendbares Recht und Gerichtsstand

Es gilt das Recht der **Bundesrepublik Deutschland** unter Ausschluss des UN-Kaufrechts. Gerichtsstand für alle Streitigkeiten ist **Amberg**, sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

§ 11 — Anlage A: Technische und organisatorische Maßnahmen (TOMs)

Gemäß Art. 32 DSGVO ergreift der Auftragnehmer folgende Maßnahmen:

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

Bereich	Maßnahme
Zutrittskontrolle	Server-Hardware betreibt der Auftragnehmer nicht selbst; alle Verarbeitung erfolgt bei Cloud-Anbietern (Supabase, Vercel, Bunny.net, all-inkl, Upstash), überwiegend ISO-27001-zertifiziert
Zugangskontrolle	Zugriff auf Operator-Daten erfolgt ausschließlich über authentifizierte Verbindungen (Supabase Auth, signierte JWTs); BoothPilot-interne Mitarbeiter haben einen separaten Auth-Pool (admin_users) mit bcrypt-gehashten Passwörtern und Pflicht-2FA (TOTP)
Zugriffskontrolle	Row-Level-Security (RLS) auf allen Datenbank-Tabellen erlaubt Operatoren nur Zugriff auf eigene Daten; Service-Role-Zugriff ist auf Server-Komponenten beschränkt
Trennungskontrolle	Mehrmandantenfähigkeit über operator_id Foreign Keys; logische Trennung pro Operator durch RLS



Bereich	Maßnahme
Pseudonymisierung	Audit-Logs speichern Aktor-IDs (UUIDs), nicht E-Mails als Primärschlüssel

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

Bereich	Maßnahme
Weitergabekontrolle	TLS 1.3 für alle externen Verbindungen (HTTPS), Content-Security-Policy-Header zur Vermeidung von Drittanbieter-Skripten ohne Zustimmung, HSTS preload-fähig konfiguriert
Eingabekontrolle	Alle fachlichen Aktionen werden im audit_logs mit Aktor, Aktion, Objekt und Zeitstempel protokolliert (DSGVO-Nachweispflicht)

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

Bereich	Maßnahme
Verfügbarkeitskontrolle	Cloud-Anbieter mit dokumentierten SLAs (Supabase ≥99.9 %, Vercel ≥99.99 %, Bunny.net ≥99.9 %, all-inkl ≥99.9 %); automatischer Heartbeat von Foto-Boxen für Live-Monitoring
Backup	Supabase-Postgres mit Point-in-Time-Recovery (7 Tage); tägliche Voll-Backups (90 Tage Aufbewahrung); Rechnungs-PDFs mit 10-Jahre-Lifecycle-Policy (HGB § 257)
Wiederherstellbarkeit	Daily-Restore-Tests mindestens vierteljährlich; Recovery-Time-Objective <4 Stunden, Recovery-Point-Objective <1 Stunde

11.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Bereich	Maßnahme
Datenschutz-Management	Vierteljährliche Überprüfung der TOMs durch den Auftragnehmer; Aktualisierung dieses AVV bei Änderungen
Incident-Response	Dokumentierter Incident-Response-Plan; alle Datenschutzverletzungen werden im internen Tracking-System protokolliert
Auftragskontrolle	Sub-Verarbeiter-Verträge werden mindestens einmal jährlich auf DSGVO-Konformität geprüft



11.5 Auftragskontrolle (Art. 32 Abs. 4 DSGVO)

Der Auftragnehmer dokumentiert alle Verarbeitungstätigkeiten in einem Verarbeitungsverzeichnis (Art. 30 DSGVO) und stellt dieses dem Auftraggeber auf Anfrage zur Verfügung.

§ 12 — Anlage B: Sub-Auftragsverarbeiter

Der Auftraggeber stimmt dem Einsatz folgender Sub-Auftragsverarbeiter ausdrücklich zu. Der Auftragnehmer hat mit jedem dieser Anbieter eine eigene Auftragsverarbeitungsvereinbarung (DPA) abgeschlossen.

Anbieter	Sitz	Verarbeitungszweck	Drittland-Transfer
Supabase, Inc.	USA / EU-Frankfurt-Hosting	PostgreSQL-Datenbank, Storage, Authentication	DPF + SCCs (Datenbank in EU, Konzernsitz USA)
Vercel, Inc.	USA / EU-Frankfurt (fra1-Region)	Web-Hosting für Marketing-Site, Operator-Dashboard, Operator-Subdomains, API-Endpoints	DPF + SCCs (Hosting in EU, Konzernsitz USA)
Stripe, Inc. USA / Irland	Subscription-Management für Operator-Pläne (BoothPilot ← Operator).	DPF + SCCs	
PayPal Pte. Ltd. Singapur / EU-Niederlassung Luxemburg (PayPal (Europe) S.à r.l. et Cie, S.C.A.)	Vermittlung von Endkunden-Zahlungen (Order-Erstellung, Webhook-Empfang). Geld fließt direkt zwischen Endkunde und Operator — BoothPilot ist nicht Treuhand.	innerhalb EU (Luxemburg-Niederlassung)	
Resend, Inc.	USA	Transaktions-E-Mail-Versand (Magic-Links, Welcome-Mails, Trial-Reminder, Rechnungs-Email)	DPF + SCCs (EU-Region beim Versand)
BunnyWay d.o.o. (Bunny.net)	Slowenien (EU); Storage-Region Falkenstein, DE	CDN + Edge-Storage für Kiosk-Software-Updates (updates.boothpilot.app); CDN-Zugriffslogs (IP)	innerhalb EU/EWR
ALL-INKL.COM – Neue Medien Münnich	Deutschland (Friedersdorf)	E-Mail-Postfach hallo@boothpilot.de + DNS-Zone boothpilot.de	innerhalb EU
Upstash, Inc.	USA / EU-Frankfurt-Hosting	Cron-Job-Scheduling, Rate-Limiting (Redis)	DPF + SCCs (Daten in EU)
Cloudflare, Inc.	USA / weltweit	Bot-Schutz (Turnstile), CDN	DPF + SCCs



Anbieter	Sitz	Verarbeitungszweck	Drittland-Transfer
Sentry, Inc. USA	Error-Tracking, Performance-Monitoring	DPF + SCCs	
Sanity, Inc.	Norwegen	CMS für Marketing-Blog (boothpilot.de/blog)	innerhalb EWR
Anthropic, PBC USA	KI-Chatbot auf Operator-Websites	SCCs (Art. 46 Abs. 2 lit. c DSGVO)	
OpenRouteService	Deutschland (HeiGIT)	Distanzberechnung für Lieferzonen	innerhalb EU
Microsoft / Azure Trusted Signing	USA / EU	Code-Signing für Windows-Installer	DPF + SCCs (administrative Daten)

Akzeptanz-Hinweis

Mit Klick auf „Akzeptieren und fortfahren“ im Onboarding-Wizard bestätigt der Auftraggeber:

1. Diesen AVV in der Version 2026-07 vollständig gelesen und verstanden zu haben
2. Mit dem Einsatz der in Anlage B genannten Sub-Auftragsverarbeiter (insbesondere Vercel und PayPal) einverstanden zu sein
3. Dass der Vertragsschluss mit Zeitstempel, Vertragsversion, IP-Adresse und User-Agent in der BoothPilot-Datenbank protokolliert wird

Eine Kopie des akzeptierten AVV-Textes kann jederzeit im Operator-Dashboard unter „Konto → Verträge“ eingesehen oder als PDF heruntergeladen werden.

