

Fassung 2 · Stand Oktober 2026 · veröffentlicht am 01.10.2026 · gilt für alle Konten ab 15.10.2026

Prüfsumme (SHA-256): d0e091d92bea309030d806bc4559b66dcd496241caf59ace5e7288af73ca4720

Abrufbar unter: <https://vizitcard.de/legal/avv/2026-10>

Vertrag zur Auftragsverarbeitung (AVV)

Gemäß Art. 28 DSGVO · für B2B-/Agentur-Kunden · Stand: Oktober 2026

Präambel und Parteien

Dieser Vertrag zur Auftragsverarbeitung (nachfolgend „Vertrag“) konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Nutzung der Plattform vizitcard.de. Er gilt für alle Verarbeitungen personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen durchführt.

Auftragsverarbeiter:

PiXX Media, Inhaber Manuel Zagler, Schillerstraße 32, 84544 Aschau am Inn, Deutschland, E-Mail: info@vizitcard.de (nachfolgend „Auftragsverarbeiter“).

Verantwortlicher: der jeweilige Agentur- bzw. Geschäftskunde, der den Dienst zur Verwaltung von Karten und der damit verbundenen personenbezogenen Daten Dritter nutzt (nachfolgend „Verantwortlicher“). Der Verantwortliche schließt diesen Vertrag mit Annahme des Angebots bzw. mit Buchung eines entsprechenden Tarifs.

Bei Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen der Parteien gehen die Regelungen dieses Vertrags in datenschutzrechtlichen Fragen vor.

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

(1) Gegenstand des Auftrags ist die Erbringung der vizitcard-Dienste gemäß dem zugrunde liegenden Hauptvertrag bzw. den AGB.

(2) Art, Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Sie endet mit dessen Beendigung, vorbehaltlich der Regelungen zur Löschung und Rückgabe (§ 9).

(4) Die Verarbeitung findet grundsätzlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums statt. Soweit einzelne, in **Anlage 3** ausdrücklich gekennzeichnete Zusatzfunktionen Anbieter mit Verarbeitung in einem Drittland einbeziehen (derzeit: automatisierte Bildprüfung, Wallet-Pässe), erfolgt die Übermittlung ausschließlich auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO – EU-US Data Privacy Framework) oder geeigneter Garantien nach Art. 46 DSGVO (EU-Standardvertragsklauseln). Im Übrigen erfolgt eine Verarbeitung in einem Drittland nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Der Verantwortliche kann die Deaktivierung der drittlandbezogenen Zusatzfunktionen für seine Karten verlangen; die übrigen Verarbeitungen bleiben davon unberührt.

§ 2 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO), es sei denn, er ist gesetzlich zu einer Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die im Rahmen der Funktionsnutzung getroffenen Konfigurationen und Einstellungen des Verantwortlichen gelten als Weisungen. Darüber hinausgehende Einzelweisungen sind in Textform zu erteilen.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis sie bestätigt oder geändert wird.

§ 3 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit:** Der Auftragsverarbeiter verpflichtet die zur Verarbeitung befugten Personen zur Vertraulichkeit oder stellt sicher, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO).

(2) **Datensicherheit:** Er trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen gemäß **Anlage 2** und hält diese auf dem Stand der Technik.

(3) **Unterstützung des Verantwortlichen:** Er unterstützt den Verantwortlichen im Rahmen des Möglichen bei der Beantwortung von Anträgen betroffener Personen (Art. 12–23 DSGVO) sowie bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Datensicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation der Aufsichtsbehörde).

(4) **Meldung von Datenschutzverletzungen:** Er meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden und stellt die zur Erfüllung der Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO) erforderlichen Informationen bereit.

(5) **Betroffenenrechte:** Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er das Anliegen unverzüglich an den Verantwortlichen weiter.

(6) **Datenschutzkonforme Gestaltung:** Der Auftragsverarbeiter berücksichtigt die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO), insbesondere durch Datenminimierung (z. B. keine Speicherung von IP-Adressen in der Reichweitenmessung).

§ 4 Pflichten des Verantwortlichen

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich. Er stellt insbesondere sicher, dass für die von ihm über den Dienst erhobenen und verwalteten Daten (z. B. Karten-, Kontakt-, Lead- und Terminiendaten der von ihm betreuten Endkunden) eine wirksame Rechtsgrundlage besteht und die erforderlichen Informationspflichten erfüllt sind.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter ergeben sich aus **Anlage 3**.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern und räumt ihm das Recht ein, gegen solche Änderungen aus wichtigem datenschutzrechtlichem Grund innerhalb einer angemessenen Frist Einspruch zu erheben (Art. 28 Abs. 2 DSGVO).

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO).

§ 6 Kontroll- und Nachweisrechte (Audit)

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen – durch den Verantwortlichen oder einen von diesem beauftragten Prüfer und trägt zu diesen bei (Art. 28 Abs. 3 lit. h DSGVO).

(2) Nachweise können vorrangig durch Vorlage geeigneter Dokumentationen, Bescheinigungen oder Zertifizierungen erbracht werden. Vor-Ort-Kontrollen erfolgen mit angemessener Vorankündigung, zu üblichen Geschäftszeiten und so, dass der Geschäftsbetrieb möglichst wenig beeinträchtigt wird.

§ 7 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, in der Regel innerhalb von 48 Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten, die die im Auftrag verarbeiteten Daten betrifft, und unterstützt ihn bei den erforderlichen Maßnahmen.

§ 8 Berichtigung, Einschränkung und Löschung im laufenden Auftrag

Der Auftragsverarbeiter berichtigt, löscht oder schränkt die Verarbeitung der Auftragsdaten nur nach Weisung des Verantwortlichen ein. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter.

§ 9 Löschung und Rückgabe nach Beendigung

Nach Abschluss der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO). Dem Verantwortlichen steht hierfür insbesondere die Exportfunktion zur Verfügung; nach Ablauf einer angemessenen Frist werden die Daten gelöscht.

§ 10 Haftung

Für die Haftung im Außenverhältnis gilt Art. 82 DSGVO. Im Innenverhältnis gelten ergänzend die Haftungsregelungen des Hauptvertrags bzw. der AGB; Haftungsbeschränkungen gelten, soweit gesetzlich zulässig, auch im Rahmen dieses Vertrags.

§ 11 Schlussbestimmungen

(1) Es gilt deutsches Recht. Änderungen und Ergänzungen bedürfen der Textform.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1 – Gegenstand und Einzelheiten der Verarbeitung

Art der Verarbeitung: Erheben, Speichern, Organisieren, Strukturieren, Anzeigen/Bereitstellen, Übermitteln (an den Verantwortlichen), Löschen.

Zweck: Bereitstellung und Betrieb digitaler Visitenkarten sowie der damit verbundenen Funktionen (öffentliche Kartenseite, QR/NFC, vCard, Reichweitenmessung, Lead-/Terminformulare, Live-Chat auf Karten, Speisekarte mit Bestellfunktion und Tischservice, Tischreservierung, Produkte und Vorbestellung — einschließlich vom Verantwortlichen selbst erfasster Vorbestellungen, etwa nach telefonischer Bestellung — sowie Hinweise und Angebote in den E-Mails an Gäste und Kunden samt Einholung (Double-Opt-in), Nachweis und Widerruf der Einwilligungen sowie Kanäle der Nachrichtenzentrale — Empfang von

Nachrichten aus vom Verantwortlichen angebundenen Systemen und Übermittlung seiner Antworten an eine von ihm bestimmte Adresse) im Auftrag des Verantwortlichen.

Art der personenbezogenen Daten: Stammdaten (z. B. Name, Position, Firma), Kontaktdaten (z. B. Telefon, E-Mail, Adresse, Profil-/Social-Links), Profil-/Bilddaten, Nutzungs- und Zugangsdaten, sowie über Kontakt-/Lead-/Terminformulare übermittelte Daten (z. B. Name, E-Mail, Telefon, Nachricht, Terminwunsch), Live-Chat-Nachrichten samt Zeitpunkten und — bei Einbettung auf einer fremden Webseite — der Herkunftsseite sowie — bei aktivierter Bestellfunktion — Bestelldaten von Gästen (z. B. Name, Telefon, E-Mail, bestellte Positionen, Anmerkungen, Abhol- bzw. Tischangabe) sowie — bei aktivierter Tischreservierung — Reservierungsdaten von Gästen (Name, Telefon, E-Mail, Zeitpunkt, Personenzahl, Bereichswunsch, Gastwunsch/Anmerkung) sowie — bei aktivierter Vorbestellung — Bestelldaten von Kunden (Name, Telefon, E-Mail, bestellte Positionen und Mengen, Anmerkungen, Abholtermin, bei Lieferung die Lieferanschrift, Stand und Änderungsverlauf der Bestellung) sowie — bei eingerichteten Kanälen der Nachrichtenzentrale — die darüber übermittelten Nachrichten samt Absenderangaben (Name, E-Mail, Telefon, soweit übermittelt), Gesprächs- und Nachrichtenkennungen des angebundenen Systems, Herkunftsseite, Zeitpunkte und Zustellstand der Antworten sowie — soweit Gäste oder Kunden in Angebote per E-Mail einwilligen — Einwilligungsnachweise (Prüfwert der E-Mail-Adresse statt der Adresse selbst, Prüfwert des Bestätigungscode, gezeigter Wortlaut und Fassung der Erklärung, die dabei geltende Fassung der Datenschutzerklärung, Sprache, Herkunft, Zeitpunkte von Anforderung, Bestätigungsmail und Bestätigung, gegebenenfalls Zeitpunkt und Weg des Widerrufs; keine IP-Adressen) sowie die Inhalte und Versandprotokolle der E-Mails an Gäste und Kunden. Zahlungsdaten sind nicht Gegenstand des Auftrags: Gastbestellungen und Vorbestellungen werden ausschließlich vor Ort beim Verantwortlichen bezahlt, und eine Tischreservierung ist für den Gast kostenlos (keine Kautions, kein Entgelt für nicht wahrgenommene Reservierungen).

Angebote in E-Mails: Der Auftragsverarbeiter stellt das freiwillige, nicht vorausgewählte Einwilligungs-Häkchen, die gesonderte, werbefreie Bestätigungsmail (Double-Opt-in) samt Bestätigungsseite, den Nachweis, den Abmeldelink in jeder E-Mail mit Angebot und die Umsetzung des Widerrufs technisch bereit; Angebote erhalten nur Empfänger, die ihre Einwilligung per Bestätigungslink bestätigt und nicht widerrufen haben. Öffnungs- oder Klickmessung findet nicht statt. Der Verantwortliche entscheidet, ob und welche Hinweise und Angebote in E-Mails erscheinen, und steht für deren Inhalt ein (insbesondere Preisangaben nach der Preisangabenverordnung und Bildrechte) sowie für die Information der Betroffenen in seiner eigenen Datenschutzerklärung. Hinweise und eigene Zusatztexte, die ohne Einwilligung an alle Empfänger gehen, dürfen keine Werbung enthalten; der Verantwortliche bestätigt das bei jedem Speichern, andernfalls erscheinen sie in keiner E-Mail. Einwilligungen kann der Verantwortliche nicht selbst für Betroffene erteilen, auch nicht bei selbst erfassten Bestellungen. Nicht bestätigte Anforderungen und die Versandprotokolle der Bestätigungs-mails werden nach 30 Tagen gelöscht, Einwilligungsnachweise nach einem Widerruf 3 Jahre aufbewahrt und danach gelöscht.

Kanäle der Nachrichtenzentrale: Der Verantwortliche entscheidet, welche Systeme er anbindet, welche Daten er darüber einspeist und an welche Adresse Antworten übermittelt werden; die Übermittlung an diese Adresse erfolgt auf seine Weisung. Der Auftragsverarbeiter nimmt nur Aufrufe mit dem geheimen Kanalschlüssel an (auf Wunsch zusätzlich mit HMAC-Signatur), speichert keine IP-Adressen der aufrufenden Systeme, übermittelt Antworten ausschließlich verschlüsselt (HTTPS) und signiert an öffentlich erreichbare Adressen und löscht Kanal-Gespräche 90 Tage nach der letzten Nachricht. Für die Rechtsgrundlage der Einspeisung und die Information der Absender ist der Verantwortliche verantwortlich; das angebundene System und der Empfänger der Antworten sind keine Unterauftragsverarbeiter des Auftragsverarbeiters.

Inhalte der E-Mails an Gäste und Kunden: Der Auftragsverarbeiter leert die gespeicherten Inhalte dieser E-Mails automatisiert, spätestens nach der Höchstfrist, die für die Bestell- bzw. Reservierungsdaten des jeweiligen Moduls gilt (bei Reservierungen bereits mit dem Löschen der Freitexte); Empfänger, Betreff und Zeitpunkt bleiben als Versandnachweis.

Kategorien betroffener Personen: Endkunden/Karteninhaber des Verantwortlichen, Besucher, Kontakthanfänger, Chat-Teilnehmer, bestellende Gäste, Vorbesteller (auch solche, deren Bestellung der

Verantwortliche selbst erfasst) und Reservierungsgäste der veröffentlichten Karten, Empfänger von Bestätigungsmails zur Einwilligung in Angebote sowie Absender von Nachrichten, die der Verantwortliche über Kanäle der Nachrichtenzentrale einspeist.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand des Auftrags, **soweit der Verantwortliche sie nicht selbst über Freitextfelder erhebt**; der Auftragsverarbeiter weist Gäste an den betreffenden Feldern ausdrücklich darauf hin, keine Gesundheitsangaben zu machen, und löscht Freitexte — samt den Inhalten der dazu versandten E-Mails — sieben Tage nach dem Termin. Im Übrigen stellt der Verantwortliche sicher, dass solche Daten nicht über den Dienst verarbeitet werden.

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

- **Vertraulichkeit:** Zugriffskontrolle über individuelle Konten und Rollen/Berechtigungen; mandantengetrennte Sichtbarkeit (Scope-Trennung B2C/Agentur); Passwörter und PINs ausschließlich als Argon2id-Hash; CSRF-Schutz und Rate-Limiting an sicherheitsrelevanten Endpunkten.
- **Integrität:** verschlüsselte Übertragung (TLS); ausschließlich vorbereitete SQL-Anweisungen; Prüfung jedes Uploads vor der Ablage — Bilder werden neu kodiert und dabei von Metadaten (EXIF) befreit, PDF-Dokumente werden nicht neu kodiert, sondern strukturell geprüft und bei aktiven Inhalten (z. B. JavaScript, eingebettete Dateien) zurückgewiesen; Ablage außerhalb des öffentlich erreichbaren Verzeichnisses unter Zufallsnamen, Auslieferung ausschließlich über eigene Endpunkte mit fester Inhaltsart — bei Dokumenten zusätzlich mit Prüfung von Veröffentlichung, Tarif und PIN; Sicherheits-Header (u. a. CSP, HSTS).
- **Verfügbarkeit und Belastbarkeit:** Betrieb auf Servern in der EU; regelmäßige Datensicherung; Protokollierung sicherheitsrelevanter Ereignisse (Audit-Log).
- **Datenminimierung:** cookieless Reichweitenmessung ohne Speicherung der IP-Adresse (sofortige Anonymisierung); lokale Geo-Datenbank ohne externen Aufruf; keine externen Tracking-Dienste.
- **Verfahren zur regelmäßigen Überprüfung:** Trennung von Test-/Produktivdaten, Pflege der eingesetzten Komponenten, Überprüfung der Wirksamkeit der Maßnahmen.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

- Hosting-/Server-Dienstleister (Standort EU/Deutschland) – Bereitstellung der Server-Infrastruktur.
- E-Mail-Versanddienst (Standort EU) – Versand transaktionsbezogener Nachrichten.
- Stripe Payments Europe Ltd., Dublin/Irland – Zahlungsabwicklung (im Umfang der Zahlungsdaten; insoweit teilweise eigene Verantwortlichkeit).
- Bei Bestellung physischer Produkte: Versand-/Logistikdienstleister (u. a. DHL) – Zustellung und Sendungsverfolgung.
- **OpenAI Ireland Limited, Dublin/Irland** (technische Verarbeitung durch OpenAI, L.L.C., San Francisco/USA) – automatisierte Prüfung hochgeladener Bilder auf unzulässige Inhalte und auf Anzeichen fremden Bildmaterials. Übermittelt wird ausschließlich das jeweilige Bild; nach den API-Bedingungen erfolgt keine Nutzung zu Trainingszwecken. *Drittlandbezug (USA)* – Grundlage: Art. 45 bzw. 46 DSGVO (siehe § 1 Abs. 4). Die Funktion ist nur aktiv, wenn die Bildprüfung im Dienst konfiguriert ist.
- **Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland** (ggf. Google LLC, USA) – Erstellung und Bereitstellung von Wallet-Pässen (Google Wallet), sofern ein Karteninhaber oder Kartenbesucher einen Pass anlegt; übermittelt werden die auf dem Pass angezeigten Karten- und Kontaktdaten. Optional zusätzlich der Abruf öffentlicher Google-Bewertungen zu einem vom Verantwortlichen hinterlegten Standort. *Drittlandbezug (USA)* – Grundlage: Art. 45 DSGVO (EU-US Data Privacy Framework). Die Funktion ist nur aktiv, wenn sie im Dienst konfiguriert und für die Karte aktiviert ist.

- Rechnungssoftware **Invoice Ninja** – vom Auftragsverarbeiter auf eigener Infrastruktur in der EU selbst betrieben (Rechnungs- und Stammdaten des Verantwortlichen); eine Weitergabe an den Softwarehersteller findet nicht statt.
- Helpdesk-Software **Zammad** – vom Auftragsverarbeiter auf eigener Infrastruktur in der EU selbst betrieben; verarbeitet die im Support-Chat bzw. Ticketformular übermittelten Daten (Name, E-Mail, Nachricht).

Die konkrete Firmierung und Anschrift der eingesetzten Unterauftragsverarbeiter wird dem Verantwortlichen auf Anfrage mitgeteilt und bei Änderungen gemäß § 5 aktualisiert.