Fassung 7 · Stand Oktober 2026 (6) · veröffentlicht am 16.10.2026 · gilt für Neukunden seit 16.10.2026

Prüfsumme (SHA-256): 2190f5d57511fa22a766185d0faf9658bce5b1cf4bdbd8563034c2d4b978df8d

Abrufbar unter: https://vizitcard.de/legal/avv/oktober-2026-6

Vertrag zur Auftragsverarbeitung (AVV)

Gemäß Art. 28 DSGVO · für Kunden, in deren Auftrag wir personenbezogene Daten verarbeiten (insbesondere B2B- und Agentur-Kunden) · Stand: Oktober 2026 (6)

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 Kunde (Nutzer des Dienstes), soweit er den Dienst zur Verarbeitung personenbezogener Daten Dritter nutzt – insbesondere als Agentur- oder Geschäftskunde für die Karten seiner Endkunden oder als Karteninhaber für Daten, die Besucher über Funktionen seiner Karten übermitteln (nachfolgend „Verantwortlicher"). Der Verantwortliche schließt diesen Vertrag mit Annahme des Angebots bzw. mit Buchung eines Tarifs, spätestens mit der Aktivierung einer Funktion, bei der der Auftragsverarbeiter in seinem Auftrag personenbezogene Daten verarbeitet.

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 und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen ergeben sich aus **Anlage 1**. Welche Verarbeitungen im Einzelnen stattfinden, bestimmt der Verantwortliche, indem er Funktionen aktiviert und einstellt (§ 2 Abs. 2). Funktionen, die nach Abschluss dieses Vertrags hinzukommen, sind vom Auftrag umfasst, soweit sie sich innerhalb der Zwecke, Datenarten und Kategorien betroffener Personen nach Anlage 1 halten; einer Änderung dieses Vertrags bedarf es dafür nicht. Funktionen, die über die vom Verantwortlichen bereits genutzten hinaus personenbezogene Daten Dritter verarbeiten, setzt der Auftragsverarbeiter erst ein, nachdem der Verantwortliche sie aktiviert hat.

(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, erfolgt die Übermittlung ausschließlich auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO, z. B. EU-US Data Privacy Framework) oder geeigneter Garantien nach Art. 46 DSGVO (z. B. EU-Standardvertragsklauseln). Im Übrigen erfolgt eine Verarbeitung in einem Drittland nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftragsverarbeiter sie nach § 5 Abs. 2 angekündigt hat. 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 Aktivierung von Funktionen sowie die im Rahmen der Funktionsnutzung getroffenen Konfigurationen und Einstellungen des Verantwortlichen gelten als dokumentierte Weisungen. Das gilt auch für die im Dienst voreingestellten Lösch- und Anonymisierungsfristen, soweit der Verantwortliche sie nicht – wo vorgesehen – ändert oder Daten früher löscht. Verlängert der Auftragsverarbeiter eine voreingestellte Frist, gilt das als Änderung nach § 11 Abs. 4. 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 nach § 7 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) und automatische Löschfristen.

§ 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, eingestellten, selbst erfassten oder über angebundene Systeme eingespeisten Daten eine wirksame Rechtsgrundlage besteht, dass die erforderlichen Informationspflichten (Art. 13 und 14 DSGVO) erfüllt sind – etwa in seiner eigenen Datenschutzerklärung – und dass erforderliche Einwilligungen vorliegen. Er beachtet die besonderen Regeln in Anlage 1.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die eingesetzten Unterauftragsverarbeiter

ergeben sich aus **Anlage 3**.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage im Voraus in Textform (z. B. per E-Mail oder im Kundenkonto) über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund Einspruch erheben (Art. 28 Abs. 2 DSGVO). Die Parteien bemühen sich dann um eine einvernehmliche Lösung; kommt keine zustande, kann der Verantwortliche die betroffene Funktion deaktivieren oder den Hauptvertrag zum Zeitpunkt der Änderung kündigen. Ist die Ersetzung wegen eines Ausfalls oder aus Sicherheitsgründen kurzfristig erforderlich, darf die Frist so weit wie nötig verkürzt werden; der Auftragsverarbeiter informiert dann unverzüglich, die Rechte nach Satz 2 und 4 bleiben unberührt. Dasselbe gilt, wenn ein Unterauftragsverarbeiter weitere Unterauftragsverarbeiter mit kürzerem Vorlauf ankündigt: Der Auftragsverarbeiter informiert unverzüglich nach Kenntnis.

(3) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind: Software, die der Auftragsverarbeiter selbst betreibt (z. B. sein E-Mail-Server sowie Rechnungs-, Helpdesk- oder Analysesoftware); Dienste, die der Verantwortliche selbst anbindet oder deren Anbieter er selbst beauftragt (z. B. eigene Kalender, Webhooks, Kanäle, Schnittstellen, Zahlungsterminals, Empfänger von Weiterleitungen); Push-Dienste der Hersteller von Browsern, Betriebssystemen und Wallet-Anwendungen, über die Benachrichtigungen an von den Empfängern selbst gewählte Geräte zugestellt werden; reine Telekommunikations- und Transportleistungen; sowie Dienstleister, die der Auftragsverarbeiter für Leistungen einsetzt, die er gegenüber dem Verantwortlichen als eigener Verantwortlicher erbringt (z. B. Zahlungsabwicklung und Versand bestellter Produkte; siehe Datenschutzerklärung).

(4) 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 (§ 2 Abs. 2). 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 Änderungen dieses Vertrags, Schlussbestimmungen

(1) Neue Funktionen im Rahmen von Anlage 1 sind keine Änderung dieses Vertrags (§ 1 Abs. 2).

(2) Der Auftragsverarbeiter darf die technischen und organisatorischen Maßnahmen (Anlage 2) an den Stand der Technik und an Änderungen des Dienstes anpassen und durch gleichwertige oder wirksamere Maßnahmen ersetzen; das Schutzniveau der vereinbarten Maßnahmen darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert er; auf Anfrage legt er sie dem Verantwortlichen dar.

(3) Für Unterauftragsverarbeiter gilt § 5. Rein beschreibende Angaben in Anlage 3, die weder einen Unterauftragsverarbeiter hinzufügen oder ersetzen noch den Ort der Verarbeitung in ein anderes Land verlegen (z. B. geänderte Anschrift oder Kontaktdaten, ein anderes Rechenzentrum desselben Unterauftragsverarbeiters im selben Land), aktualisiert der Auftragsverarbeiter ohne Vertragsänderung.

(4) Sonstige Änderungen dieses Vertrags teilt der Auftragsverarbeiter dem Verantwortlichen mindestens 30 Tage vor ihrem Wirksamwerden in Textform mit. Widerspricht der Verantwortliche nicht innerhalb dieser Frist, gelten die Änderungen als genehmigt; hierauf wird in der Mitteilung gesondert hingewiesen. Im Falle eines Widerspruchs kann jede Partei den Hauptvertrag zum Wirksamwerden der Änderung kündigen. Änderungen, die das Schutzniveau für die Auftragsdaten senken, werden nur mit ausdrücklicher Zustimmung des Verantwortlichen wirksam. Im Übrigen bedürfen Änderungen und Ergänzungen der Textform.

(5) Es gilt deutsches Recht. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1 – Gegenstand und Einzelheiten der Verarbeitung

Art der Verarbeitung: Erheben, Erfassen, Speichern, Organisieren, Strukturieren, Anpassen, Auslesen, Abfragen, Anzeigen und Bereitstellen, Übermitteln (an den Verantwortlichen und an von ihm bestimmte Empfänger), Abgleichen, Einschränken, Anonymisieren und Löschen.

Zwecke – jeweils im Umfang der vom Verantwortlichen aktivierten Funktionen:

1. Bereitstellung, Veröffentlichung und Verwaltung von Karten und ihren Inhalten (einschließlich Angaben zu Endkunden, Beschäftigten und sonstigen Personen, die der Verantwortliche einstellt), ihre Verteilung per QR-Code, NFC, vCard und Wallet-Pass sowie die Verwaltung von Karten für Endkunden durch Agenturen (Übergabe, Import);
2. Reichweiten- und Nutzungsstatistik der Karten für den Verantwortlichen;
3. Entgegennahme, Verwaltung und Beantwortung von Anfragen und Nachrichten, z. B. über Kontakt-, Lead-, Termin- oder Rückrufformulare, den Live-Chat und die Nachrichtenzentrale einschließlich ihrer Kanäle (Empfang aus vom Verantwortlichen angebundenen Systemen, Übermittlung seiner Antworten an von ihm bestimmte Adressen);
4. Abwicklung von Vorgängen mit Gästen und Kunden des Verantwortlichen, z. B. Bestellungen (auch vom Tisch, mit Kellnerruf und Tischservice), Vorbestellungen (auch vom Verantwortlichen selbst erfasste), Reservierungen, Termin- und Veranstaltungsanmeldungen, einschließlich der Abstimmung mit vom Verantwortlichen angebundenen Systemen (z. B. seinem Kalender);

5. Rückmeldungen und Kundenbindung, z. B. Umfragen, Bewertungsanfragen, Stempelkarten sowie Ausgabe und Einlösung von Gutscheinen und Prämien;
6. Nachrichten an Gäste und Kunden im Namen des Verantwortlichen (z. B. Bestätigungen, Statusmitteilungen, Erinnerungen, Benachrichtigungen) einschließlich darin enthaltener Hinweise des Verantwortlichen und – nur mit Einwilligung – Angebote, samt Einholung (Double-Opt-in), Nachweis und Widerruf dieser Einwilligungen;
7. Verwaltung von Kontakten, die der Verantwortliche selbst erfasst, einscannt, importiert oder von Karten der Plattform übernimmt (z. B. gesammelte Visitenkarten), einschließlich ihrer Aktualisierung aus übernommenen Karten, ihrer Ausgabe als Datei oder QR-Code und ihres Abgleichs mit Geräten und Adressbüchern des Verantwortlichen;
8. Prüfung der vom Verantwortlichen benannten Websites auf Auffindbarkeit (Abruf öffentlich erreichbarer Seiten in Auszügen, Auswertung, Berichte, Verlauf und Maßnahmen für den Verantwortlichen), einschließlich der Auswertung von Angaben und Dateien, die der Verantwortliche dazu liefert;
9. KI-gestützte Funktionen auf Anforderung des Verantwortlichen (z. B. Vorschläge zur Gestaltung von Drucksachen und Karten oder zu Texten): Übermittlung seiner Eingabe und der dafür benötigten Inhalte an KI-Dienstleister (Anlage 3), beschränkt auf das für die Funktion Nötige; keine Speicherung von Eingaben und Antworten beim Auftragsverarbeiter, soweit die Funktion nichts anderes vorsieht;
10. Schutz der vorgenannten Funktionen vor Missbrauch und Angriffen (z. B. kurzlebige Zähler über Prüfwerte statt gespeicherter IP-Adressen).

Art der personenbezogenen Daten:

- Stamm- und Kontaktdaten (z. B. Name, Position, Firma, Telefon, E-Mail, Anschrift, Profil- und Social-Links) sowie Bild- und Dokumentdaten der Karteninhalte;
- Inhalte von Anfragen, Nachrichten und Gesprächen samt Absenderangaben, Zeitpunkten, Sprache, Herkunftsseite, Kennungen angebundener Systeme und Zustellstand;
- Vorgangsdaten (z. B. bestellte Positionen, Mengen, Beträge, Anmerkungen, Termine, Zeitpunkte, Personenzahl, Tisch- und Bereichsangaben, Abhol- und Lieferangaben einschließlich Lieferanschrift, Stand und Änderungsverlauf eines Vorgangs);
- Antworten auf Umfragen (Auswahl, Bewertungen, Zahlen, Datumsangaben, Freitexte) und zugehörige Metadaten (z. B. gerundeter Zeitpunkt, Sprache, Herkunft des Aufrufs) sowie Gutschein-, Stempel- und Einlösedaten;
- Einwilligungs- und Nachweisdaten (z. B. Prüfwerte statt E-Mail-Adressen, gezeigter Wortlaut und seine Fassung, Zeitpunkte von Anforderung, Bestätigung und Widerruf);
- Angaben zu Kontakten, die der Verantwortliche sammelt (z. B. Stamm- und Kontaktdaten, Geburtstag, Notizen, Stichwörter, Datum und Anlass des Kennenlernens, Herkunft des Eintrags) sowie Fotos von Visitenkarten;
- Inhalte und Versandprotokolle von E-Mails und Benachrichtigungen an Gäste und Kunden sowie Push-Abonnements, die Empfänger selbst einrichten;
- Inhalte der vom Verantwortlichen benannten Websites in Auszügen (z. B. Seitentitel, Beschreibungen, Überschriften, kurze Textproben, Linkziele, Angaben aus Impressum, Kontakt- oder Teamseiten) sowie Angaben und Auswertungen, die der Verantwortliche zur Prüfung liefert;
- Nutzungs- und Zugangsdaten (z. B. Statistikdaten ohne gespeicherte IP-Adressen, Erreichbarkeitsstatus, Zugänge und Geräte-Links, die der Verantwortliche vergibt).

Zahlungs- und Kartendaten von Gästen und Kunden sind nicht Gegenstand des Auftrags. Löst der Verantwortliche über den Dienst eine Zahlung an einem eigenen Zahlungsterminal aus, verarbeitet der Auftragsverarbeiter dazu nur Vorgangsdaten (z. B. Betrag, Status, Kennung des Zahlungsvorgangs), keine Kartendaten.

Kategorien betroffener Personen: Endkunden und Karteninhaber des Verantwortlichen sowie Beschäftigte und sonstige Personen, deren Angaben auf Karten stehen; Besucher der Karten; Personen, die über

Funktionen der Karten Anfragen, Nachrichten, Bestellungen, Vorbestellungen, Reservierungen, Terminwünsche oder Umfrageantworten übermitteln oder Gutscheine, Stempelkarten und Wallet-Pässe nutzen – einschließlich Personen, deren Angaben der Verantwortliche selbst erfasst oder über angebundene Systeme einspeist (Gäste, Kunden, Interessenten); Personen, deren Kontaktdaten der Verantwortliche sammelt (z. B. Geschäftskontakte, deren Visitenkarten er einscannt, importiert oder von Karten der Plattform übernimmt); Empfänger von Nachrichten im Namen des Verantwortlichen; Personen, denen der Verantwortliche Zugänge einräumt (z. B. Personal mit Geräte-Links); Personen, deren Angaben auf den vom Verantwortlichen benannten Websites stehen (z. B. Beschäftigte, Autoren, Ansprechpartner).

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand des Auftrags, **soweit der Verantwortliche sie nicht selbst über Freitextfelder erhebt**. Der Auftragsverarbeiter weist an Freitextfeldern, bei denen das naheliegt (z. B. Wünsche zu einer Reservierung), ausdrücklich darauf hin, keine Gesundheitsangaben zu machen, und löscht solche Freitexte, wo die Funktion es vorsieht, vorzeitig. Im Übrigen stellt der Verantwortliche sicher, dass solche Daten nicht über den Dienst verarbeitet werden.

Löschung: Der Dienst löscht bzw. anonymisiert Auftragsdaten automatisiert nach den Fristen, die die jeweilige Funktion bzw. die Datenschutzerklärung des Auftragsverarbeiters nennt, soweit der Verantwortliche nicht früher löscht oder – wo vorgesehen – eine andere Frist einstellt (§ 2 Abs. 2). Inhalte von E-Mails zu Bestellungen, Vorbestellungen und Reservierungen werden spätestens mit den personenbezogenen Daten des zugehörigen Vorgangs geleert; Empfänger, Betreff und Zeitpunkt bleiben als Versandnachweis. Der Verantwortliche kann einzelne Vorgänge jederzeit löschen.

Besondere Regeln einzelner Funktionsarten

a) Werbliche Inhalte in Nachrichten an Gäste und Kunden. Angebote und sonstige Werbung des Verantwortlichen erhalten nur Empfänger, die ihre Einwilligung per Bestätigungslink (Double-Opt-in) bestätigt und nicht widerrufen haben; der Auftragsverarbeiter stellt dafür ein freiwilliges, nicht vorausgewähltes Einwilligungs-Häkchen, eine werbefreie Bestätigungsnachricht, den Nachweis, einen Abmeldelink in jeder Nachricht mit Werbung und die Umsetzung des Widerrufs bereit; eine Öffnungs- oder Klickmessung findet nicht statt. Einwilligungen kann der Verantwortliche nicht selbst für Betroffene erteilen, auch nicht bei selbst erfassten Vorgängen. Hinweise und Zusatztexte, die ohne Einwilligung an alle Empfänger gehen, dürfen keine Werbung enthalten; der Verantwortliche bestätigt das, wo die Funktion es vorsieht, beim Speichern. Er entscheidet über Inhalt und Gestaltung seiner Hinweise und Angebote und steht für sie ein (insbesondere Preisangaben und Bildrechte).

b) Umfragen und Belohnungen. Der Verantwortliche bestimmt Fragen, Dankeschön, Bedingungen und – im angebotenen Rahmen – die Aufbewahrungsdauer der Antworten. Er stellt keine Fragen nach Name, Kontaktdaten oder besonderen Kategorien personenbezogener Daten, soweit die Funktion das nicht ausdrücklich vorsieht, und steht für die Inhalte und die Lauterkeit seiner Umfrage ein (insbesondere: Dankeschön für jede vollständige Teilnahme unabhängig vom Inhalt der Antworten, keine Verlosung, keine Belohnung für Bewertungen, Jugendschutz). Der Auftragsverarbeiter holt die Einwilligung der Teilnehmenden ein, speichert zu Teilnahmen weder IP-Adressen noch Kennungen und hält Gutscheine und Antworten getrennt.

c) Angebundene Systeme und Weiterleitungen. Welche Systeme der Verantwortliche anbindet (z. B. Kanäle, Webhooks, Schnittstellen, Kalender), welche Daten er darüber einspeist und an welche Adressen Daten übermittelt werden, entscheidet er; die Übermittlung erfolgt auf seine Weisung. Der Auftragsverarbeiter nimmt Aufrufe nur mit den dafür vergebenen geheimen Schlüsseln an, speichert keine IP-Adressen der aufrufenden Systeme und übermittelt Daten an solche Adressen nur verschlüsselt (HTTPS) und, wo vorgesehen, signiert. Für die Rechtsgrundlage der Einspeisung und die Information der Betroffenen ist der Verantwortliche verantwortlich.

d) Gesammelte Kontakte. Welche Kontakte der Verantwortliche sammelt, entscheidet er; er stellt die Rechtsgrundlage und, soweit erforderlich, die Information der Betroffenen sicher (§ 4). Der Auftragsverarbeiter nimmt von sich aus keinen Kontakt zu den Betroffenen auf und wertet Fotos von Visitenkarten nicht automatisiert aus. Kontakte aus übernommenen Karten hält er nur mit den Angaben

aktuell, die der Inhaber der Karte für alle Besucher zum Speichern freigegeben hat; im Übrigen gleicht er gesammelte Kontakte nicht mit Daten anderer Kunden ab. Ruft der Verantwortliche Kontakte mit eigenen Geräten oder Programmen ab (z. B. über einen Adressbuch-Abgleich), ist er für ihre weitere Verarbeitung dort verantwortlich.

e) Prüfung benannter Websites. Welche Websites der Auftragsverarbeiter prüft, bestimmt der Verantwortliche; er benennt nur Websites, die ihm gehören oder für die er beauftragt ist, und stellt die Rechtsgrundlage für die dort veröffentlichten Angaben Dritter sicher. Der Auftragsverarbeiter ruft nur öffentlich erreichbare Seiten ab, beachtet deren Anweisungen an Abrufprogramme (robots.txt), begrenzt Zahl und Geschwindigkeit der Abrufe, speichert keine vollständigen Kopien, sondern Auszüge und Befunde, und nimmt von sich aus keinen Kontakt zu Betroffenen auf. Websites Dritter, die der Verantwortliche zum Vergleich benennt, wertet der Auftragsverarbeiter nur als Begriffsstatistik ohne personenbezogene Auszüge aus.

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

- **Vertraulichkeit:** Zugriffskontrolle über individuelle Konten und Rollen/Berechtigungen; mandantengetrennte Sichtbarkeit (Trennung von Konten, Agenturen und Endkunden); Passwörter und PINs ausschließlich als Argon2id-Hash; Passwörter und Schlüssel angebundener Dienste (z. B. Kalender, Kanäle) verschlüsselt gespeichert; 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, Dokumente strukturell geprüft und bei aktiven Inhalten zurückgewiesen; Ablage außerhalb des öffentlich erreichbaren Verzeichnisses unter Zufallsnamen, Auslieferung ausschließlich über eigene Endpunkte mit Zugriffsprüfung; Sicherheits-Header (u. a. CSP, HSTS).
- **Verfügbarkeit und Belastbarkeit:** Betrieb auf Servern in der EU; regelmäßige Datensicherung; Protokollierung sicherheitsrelevanter Ereignisse (Audit-Log).
- **Datenminimierung:** Reichweitenmessung ohne Cookies und ohne Speicherung der IP-Adresse (sofortige Anonymisierung); lokale Geo-Datenbank ohne externen Aufruf; keine externen Tracking-Dienste auf Karten ohne Einwilligung; zufällige, nicht erratbare Adressen für Status- und Verwaltungsseiten von Gästen; automatische Lösch- und Anonymisierungsfristen.
- **Verfahren zur regelmäßigen Überprüfung:** Trennung von Test- und Produktivdaten, Pflege der eingesetzten Komponenten, Überprüfung der Wirksamkeit der Maßnahmen.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

- **Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland** (Datenschutz-Kontakt: data-protection@hetzner.com) – Hosting: Bereitstellung der Server-Infrastruktur, auf der der Dienst betrieben wird, einschließlich des vom Auftragsverarbeiter selbst betriebenen E-Mail-Servers (Versand von E-Mails, z. B. Benachrichtigungen an den Verantwortlichen und Nachrichten an Gäste und Kunden). Serverstandort Deutschland, kein Drittlandbezug.
- **OpenAI Ireland Limited, Dublin/Irland** (technische Verarbeitung durch OpenAI, L.L.C., San Francisco/USA) – automatisierte Vorprüfung hochgeladener Bilder auf unzulässige Inhalte und Anzeichen fremden Bildmaterials (nur als Hinweis für die Prüfung durch Mitarbeiter des Auftragsverarbeiters; keine automatische Sperre). Übermittelt wird das jeweilige Bild, gegebenenfalls mit Name, Position und Firma als Einordnungshilfe; nach den API-Bedingungen keine Nutzung zu Trainingszwecken. *Drittlandbezug (USA)* – Grundlage: Art. 45 bzw. 46 DSGVO (§ 1 Abs. 4). Nur aktiv, wenn die Bildprüfung im Dienst eingeschaltet ist. Außerdem – nur auf Anforderung des Verantwortlichen – KI-gestützte Funktionen (Anlage 1, Zweck 9): übermittelt werden seine Eingabe und die dafür benötigten Inhalte.

- **Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland** (technische Verarbeitung durch Anthropic, PBC, San Francisco/USA) – KI-gestützte Funktionen nur auf Anforderung des Verantwortlichen (Anlage 1, Zweck 9): übermittelt werden seine Eingabe und die dafür benötigten Inhalte; nach den Vertragsbedingungen keine Nutzung zu Trainingszwecken. *Drittlandbezug (USA)* – Grundlage: Art. 45 bzw. 46 DSGVO (§ 1 Abs. 4).
- **Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland** (ggf. Google LLC, USA) – Erstellung und Aktualisierung von Wallet-Pässen (Google Wallet), sofern ein Karteninhaber oder Besucher einen Pass anlegt; übermittelt werden die auf dem Pass angezeigten Karten-, Kontakt- bzw. Stempeldaten. Optional Abruf öffentlicher Google-Bewertungen zu einem vom Verantwortlichen hinterlegten Standort. *Drittlandbezug (USA)* – Grundlage: Art. 45 DSGVO (EU-US Data Privacy Framework). Nur aktiv, wenn die Funktion im Dienst eingerichtet und für die Karte genutzt wird.

Soweit oben nicht angegeben, teilt der Auftragsverarbeiter dem Verantwortlichen Firmierung und Anschrift eines Unterauftragsverarbeiters auf Anfrage mit. Änderungen dieser Liste kündigt er nach § 5 Abs. 2 an.