Änderungen: Auftragsverarbeitungsvertrag (AVV)

Vergleich „Stand Oktober 2026 (2)" -> „Stand Oktober 2026 (3)" · erstellt am 23.11.2026 08:16

22 Stelle(n) geändert, 31 hinzugefügt, 14 entfernt.

Betroffene Abschnitte

- Vertrag zur Auftragsverarbeitung (AVV)
- Präambel und Parteien
- § 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung
- § 2 Weisungsrecht des Verantwortlichen
- § 3 Pflichten des Auftragsverarbeiters
- § 4 Pflichten des Verantwortlichen
- § 5 Unterauftragsverarbeiter
- § 8 Berichtigung, Einschränkung und Löschung im laufenden Auftrag
- § 11 Änderungen dieses Vertrags, Schlussbestimmungen
- Anlage 1 – Gegenstand und Einzelheiten der Verarbeitung
- Besondere Regeln einzelner Funktionsarten
- Anlage 2 – Technische und organisatorische Maßnahmen (TOM, Art. 32 DSGVO)
- Anlage 3 – Genehmigte Unterauftragsverarbeiter

Geänderte Stellen

Durchgestrichen = entfällt · fett grün = neu · grau = unverändertes Umfeld

Vertrag zur Auftragsverarbeitung (AVV)

Vertrag zur Auftragsverarbeitung (AVV)

Gemäß Art. 28 DSGVO · für ~~B2B-/Agentur-Kunden~~ **Kunden, in deren Auftrag wir personenbezogene Daten verarbeiten (insbesondere B2B- und Agentur-Kunden)** · Stand: Oktober 2026 ~~(2)~~ **(3)**

Präambel und Parteien

Präambel und Parteien

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~~ **Kunde (Nutzer des Dienstes), soweit er** den Dienst zur ~~Verwaltung von Karten und der damit verbundenen personenbezogenen~~ **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 ~~entsprechenden Tarifs.~~ **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,~~ **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 (derzeit: automatisierte Vorprüfung von Bildern, Wallet-Pässe),~~ **einbeziehen,** erfolgt die Übermittlung ausschließlich auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 ~~DSGVO –~~ **DSGVO, z. B.** EU-US Data Privacy Framework) oder geeigneter Garantien nach Art. 46 DSGVO ~~(EU-Standardvertragsklauseln).~~ **(z. B. EU-Standardvertragsklauseln).** Im Übrigen erfolgt eine Verarbeitung in einem Drittland nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt ~~sind.~~ **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

(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~~ **§ 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).~~ **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 und verwalteten~~ **erhobenen, eingestellten, selbst erfassten oder über angebundene Systeme eingespeisten** Daten ~~(z. B. Karten-, Kontakt-, Lead- und Termindaten der von ihm betreuten Endkunden)~~ eine wirksame Rechtsgrundlage ~~besteht und~~ **besteht, dass** die erforderlichen Informationspflichten **(Art. 13 und 14 DSGVO)** erfüllt ~~sind.~~ **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 ~~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).~~

(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.

(3) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind: Software, die der Auftragsverarbeiter selbst betreibt (z. B. 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).

~~(3)~~ **(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)

§ 8 Berichtigung, Einschränkung und Löschung im laufenden Auftrag

§ 8 Berichtigung, Einschränkung und Löschung im laufenden Auftrag

Der Auftragsverarbeiter berichtigt, löscht oder schränkt die Verarbeitung der Auftragsdaten nur nach Weisung des Verantwortlichen ~~ein.~~ **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

§ 11 Änderungen dieses Vertrags, Schlussbestimmungen

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

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

(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.

(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, ~~Anzeigen/Bereitstellen,~~ **Anpassen, Auslesen, Abfragen, Anzeigen und Bereitstellen,** Übermitteln (an den ~~Verantwortlichen),~~ **Verantwortlichen und an von ihm bestimmte Empfänger), Abgleichen, Einschränken, Anonymisieren und** 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 Bestätigungscodes, 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 Kaution, 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 Bestätigungsmails 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, Kontaktanfragende, 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.~~

Zwecke – jeweils im Umfang der vom Verantwortlichen aktivierten Funktionen:

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);

Reichweiten- und Nutzungsstatistik der Karten für den Verantwortlichen;

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);

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);

Rückmeldungen und Kundenbindung, z. B. Umfragen, Bewertungsanfragen, Stempelkarten sowie Ausgabe und Einlösung von Gutscheinen und Prämien;

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;

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);

Inhalte und Versandprotokolle von E-Mails und Benachrichtigungen an Gäste und Kunden sowie Push-Abonnements, die Empfänger selbst einrichten;

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); Empfänger von Nachrichten im Namen des Verantwortlichen; Personen, denen der Verantwortliche Zugänge einräumt (z. B. Personal mit Geräte-Links).

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.

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

Vertraulichkeit: Zugriffskontrolle über individuelle Konten und Rollen/Berechtigungen; mandantengetrennte Sichtbarkeit ~~(Scope-Trennung B2C/Agentur);~~ **(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, ~~PDF-Dokumente werden nicht neu kodiert, sondern~~ **Dokumente** 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;~~ **Zugriffsprüfung;** 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 **Cookies und ohne** Speicherung der IP-Adresse (sofortige Anonymisierung); lokale Geo-Datenbank ohne externen Aufruf; keine externen ~~Tracking-Dienste.~~ **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-/Produktivdaten,~~ **Test- und Produktivdaten,** Pflege der eingesetzten Komponenten, Überprüfung der Wirksamkeit der Maßnahmen.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

~~Hosting-/Server-Dienstleister~~ **Hosting-/Rechenzentrumsdienstleister** (Standort EU/Deutschland) – Bereitstellung der ~~Server-Infrastruktur.~~ **Server-Infrastruktur, auf der der Dienst betrieben wird.**

E-Mail-Versanddienst (Standort EU) – ~~Versand transaktionsbezogener Nachrichten.~~ **Zustellung von E-Mails, z. B. Benachrichtigungen an den Verantwortlichen und Nachrichten an Gäste und Kunden.**

~~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 Vorprüfung hochgeladener Bilder auf unzulässige Inhalte und ~~auf~~ Anzeichen fremden Bildmaterials (nur als Hinweis für die Prüfung durch ~~unsere Mitarbeiter; es erfolgt~~ **Mitarbeiter des Auftragsverarbeiters;** keine automatische Sperre). Übermittelt wird ~~ausschließlich~~ das jeweilige ~~Bild;~~ **Bild, gegebenenfalls mit Name, Position und Firma als Einordnungshilfe;** 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~~ **Nur** aktiv, wenn die Bildprüfung im Dienst ~~konfiguriert~~ **eingeschaltet** ist.

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (ggf. Google LLC, USA) – Erstellung und ~~Bereitstellung~~ **Aktualisierung** von Wallet-Pässen (Google Wallet), sofern ein Karteninhaber oder ~~Kartenbesucher~~ **Besucher** einen Pass anlegt; übermittelt werden die auf dem Pass angezeigten ~~Karten- und Kontaktdaten.~~ **Karten-, Kontakt- bzw. Stempeldaten.** 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~~ **Nur** aktiv, wenn ~~sie~~ **die Funktion** im Dienst ~~konfiguriert~~ **eingerichtet** und für die Karte ~~aktiviert ist.~~ **genutzt wird.**

~~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~~ **teilt der Auftragsverarbeiter** dem Verantwortlichen auf Anfrage ~~mitgeteilt und bei~~ **mit.** Änderungen ~~gemäß~~ **dieser Liste kündigt er nach** § 5 ~~aktualisiert.~~ **Abs. 2 an.**