

Vereinbarung zur Auftragsverarbeitung

Stand: 21. Oktober 2026

Diese Vereinbarung zur Auftragsverarbeitung (AVV) beschreibt die Verarbeitung personenbezogener Kartendaten durch die palmstudio GmbH für geschäftliche Auftraggeber von DigiVisitenkarte und DigiCard Pro. Sie umfasst die nachstehenden Standardvertragsklauseln und sämtliche Anlagen.

1. Geltung und Vertragsgrundlage

Wir bieten diese AVV mit sämtlichen Anlagen verbindlich als Bestandteil unserer [Nutzungsbedingungen](#) an. Sie wird mit dem in Anhang I bezeichneten Auftraggeber durch dessen wirksame Zustimmung zu den Nutzungsbedingungen bei Registrierung oder Bestellung vereinbart, gegebenenfalls durch eine hierzu berechtigte vertretende Person. Eine gesonderte Unterschrift, ein zusätzliches Formular oder eine weitere Annahmeerklärung durch uns ist nicht erforderlich. Die Veröffentlichung allein, ein Karteninhalt oder eine frühere Zustimmung zu einer anderen AGB-Fassung begründet dagegen keinen Abschluss dieser AVV. Die Vereinbarung wirkt nicht auf frühere Verarbeitungen zurück.

Die AVV gilt, soweit der Auftraggeber als Verantwortlicher personenbezogene Daten durch uns im Auftrag verarbeiten lässt. Sie gilt unabhängig von Kartenvariante, Anzahl, Gruppenfunktion oder Kontotyp. Eine private Nutzung ausschließlich eigener Daten begründet für sich genommen keine solche Auftragsverarbeitung. Handelt ein Kunde seinerseits als Auftragsverarbeiter, sind die Beauftragung durch den tatsächlichen Verantwortlichen und die dafür erforderlichen weiteren Vereinbarungen vor der Verarbeitung gesondert zu klären.

Der Auftraggeber entscheidet über die betroffenen Personen, die zulässigen Karteninhalte, Empfänger und Veröffentlichung. Er verantwortet die Rechtsgrundlage, erforderliche Informationen und gegebenenfalls Einwilligungen, insbesondere für Fotos und öffentliche Kartenadressen. Wir verantworten die uns als Auftragsverarbeiter obliegenden Pflichten, insbesondere weisungsgebundene Verarbeitung, Vertraulichkeit, Sicherheit und Unterstützung. Die AVV überträgt unsere eigenen gesetzlichen Pflichten nicht auf den Auftraggeber.

Wir verwenden die [Standardvertragsklauseln des Durchführungsbeschlusses \(EU\) 2021/915](#). Ausgewählt sind die DSGVO-Optionen (jeweils Option 1 in Klauseln 1, 8 und 9), die allgemeine schriftliche Genehmigung in Klausel 7.7(a) mit 30 Tagen Vorankündigung (Option 2) und keine Kopplungsklausel nach der fakultativen Klausel 5. Die übrigen Klauseln bleiben inhaltlich unverändert. Die ausgefüllten Anlagen konkretisieren den Dienst. Bei Widersprüchen haben die Standardvertragsklauseln

Vorrang, auch gegenüber Haftungs- oder sonstigen Bestimmungen unserer [Nutzungsbedingungen](#).

Diese Klauseln regeln Auftragsverarbeitung nach Artikel 28 DSGVO. Sie sind für sich genommen keine Garantie für zulässige Drittlandübermittlungen. Die dafür zusätzlich erforderlichen Grundlagen werden in Anhang IV beschrieben und müssen für die tatsächlich eingesetzten Dienste vorliegen.

2. Standardvertragsklauseln

ABSCHNITT I

Klausel 1 - Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.
- b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 - Unabänderbarkeit der Klauseln

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 - Auslegung

- a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 - Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

ABSCHNITT II - PFLICHTEN DER PARTEIEN

Klausel 6 - Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 - Pflichten der Parteien

7.1 Weisungen

- a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
- b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter

diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 30 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche - im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist - das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 - Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
 3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
 4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 - Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
 1. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3. die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III - SCHLUSSBESTIMMUNGEN

Klausel 10 - Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche - unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 - den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
2. der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

3. Anhang I - Vertragsparteien

Verantwortlicher

Verantwortlicher ist das Unternehmen, die Organisation oder der geschäftlich handelnde Einzelunternehmer, für den der zustimmende Nutzer tatsächlich und erkennbar handelt. Name beziehungsweise Firmierung und Anschrift ergeben sich aus den zugeordneten Bestell- und Rechnungsdaten; die zugehörigen Konto- oder Bestellkontaktdaten bezeichnen die handelnde Kontaktperson. Diese Angaben sowie der zugehörige Zeitpunkt der Zustimmung und die zu diesem Zeitpunkt angebotene Vertragsfassung konkretisieren diesen Anhang, ohne dass ein gesondertes Firmenformular erforderlich ist. Die vorhandenen Registrierungs-, Bestell- und Rechnungsunterlagen bilden zusammen mit der datierten Vertragsfassung den Vertragsnachweis. Bei einer abweichenden Zahlstelle bleibt der tatsächlich vertretene Auftraggeber maßgeblich; eine unklare Zuordnung ist vor der Verarbeitung zu klären. Ein bloßer Karteninhalt oder Gruppenname macht eine Stelle nicht zum Verantwortlichen. Der Nutzer muss über die erforderliche Vertretungsberechtigung verfügen; die Zustimmung schafft diese nicht.

Weisungen erteilen die im Vertragsnachweis oder später nachweisbar benannten berechtigten Personen. Die verifizierten Bedienhandlungen innerhalb ihrer jeweiligen Karten- und Gruppenberechtigungen sind dokumentierte Weisungen zur betreffenden Funktion. Zusätzliche Weisungen können in Textform an unseren Datenschutzkontakt gerichtet werden; bei Zweifeln prüfen wir die Berechtigung vor der Ausführung.

Auftragsverarbeiter

palmstudio GmbH, Pfalzgrafenstraße 38, 67434 Neustadt an der Weinstraße, Deutschland. Handelsregister: Amtsgericht Ludwigshafen am Rhein, HRB 69525. Vertreten durch den Geschäftsführer Benedikt Falkenstein. Marken: DigiVisitenkarte und DigiCard Pro.

Kontakt für Datenschutz, Weisungen und Vorfälle: support@digivisitenkarte.de oder support@digicard.pro. Ansprechpartner auf Seiten des Auftragsverarbeiters ist die Geschäftsführung; diese Funktionsadresse ist keine Behauptung, dass ein externer Datenschutzbeauftragter bestellt wurde.

Der Abschluss erfolgt elektronisch nach Abschnitt 1; sein Datum ergibt sich aus der zugehörigen Zustimmung zu den Nutzungsbedingungen. Eine spätere Änderung dieser veröffentlichten Seite ändert eine bereits vereinbarte Vertragsfassung nicht automatisch.

4. Anhang II - Beschreibung der Verarbeitung

Gegenstand, Art und Zweck

Bereitstellung und Verwaltung digitaler Visitenkarten nach den Einstellungen des Auftraggebers: Entgegennahme von Eingaben und Importdaten, Speicherung, Zusammenführung von Gruppen- oder Vorlagenvorgaben, Aufbereitung von Bildern, Erstellung und Aktualisierung von Wallet-Dateien beziehungsweise Wallet-Objekten, QR-Codes und Kontaktexporten, Bereitstellung von Online-Visitenkarten und Foto-Kontakt-Downloads sowie angeforderte Kartenzustellung per E-Mail. Hinzu kommen die dafür erforderliche Berechtigungsprüfung, Auftragsbearbeitung, technische Fehlerbehebung und Löschung.

Die Verarbeitung erfolgt automatisiert und, soweit für eine berechtigte Supportanfrage, Weisung oder Störungsbehebung erforderlich, durch befugte Personen. Wir verwenden die im Auftrag verarbeiteten Karteninhalte nicht für eigene Werbung, zum Training von KI-Modellen oder zum Aufbau eigener Kontaktverzeichnisse.

Betroffene Personen und Daten

Betroffen sind Beschäftigte, Geschäftsführung, Beauftragte und sonstige vom Auftraggeber berechtigt auf einer Karte bezeichnete Personen sowie die von ihm bestimmten Empfänger der Kartenzustellung.

Verarbeitet werden die tatsächlich bereitgestellten Namen, Anreden, beruflichen Funktionen, Unternehmenszuordnungen, E-Mail-Adressen, Telefonnummern, Geschäftsadressen, Websites, Social-Media-Kennungen und Links, Notizen, Kurzbeschreibungen, Linkbeschriftungen, Fotos, Coverbilder und gegebenenfalls personenbezogenen Logos. Hinzu kommen Gruppenzuordnung, Karten- und Assetreferenzen, Design- und QR-Einstellungen, Änderungs- und Zustellstatus, berechtigungsrelevante Zuordnungen und die für Auslieferung und Fehlerbehandlung erforderlichen technischen Daten. Bei aktivierten Wallet-Updates können Pass- und Objektkennungen sowie Apple-Geräteregistrierungen und Push-Tokens verarbeitet werden. Optionale Standortangaben beschreiben die vom Auftraggeber gesetzten Relevanzorte; eine laufende Ortung von Beschäftigten ist keine Funktion des Dienstes.

Besondere Kategorien nach Artikel 9 DSGVO und strafrechtliche Daten nach Artikel 10 DSGVO sind nicht Gegenstand des vereinbarten Standarddienstes und dürfen nicht gezielt übermittelt werden. Übliche Profilfotos werden nicht zur biometrischen Identifizierung ausgewertet. Erkennt eine Partei dennoch sensible Inhalte, informiert sie die andere und klärt unverzüglich deren Einschränkung oder Entfernung sowie gegebenenfalls zusätzliche Schutzmaßnahmen; Klausel 7.5 bleibt anwendbar.

Veröffentlichung, Empfänger und Weisungen

Die angeforderten Karten-, Gruppen-, Import-, Bild-, Export- und Zustellfunktionen bilden den vereinbarten Weisungsrahmen. Ein Offline-vCard-QR-Code enthält die Kontaktdaten unmittelbar. Online-Visitenkarten, Foto-Kontaktlinks und für Wallets bestimmte Bildadressen sind für Personen mit der jeweiligen Adresse abrufbar. Eine andere QR-Zielwahl macht diese Adressen nicht automatisch privat. Suchmaschinen werden bei Online-Visitenkarten um Nichtindexierung gebeten; dies ist keine Zugangssperre.

Der Auftraggeber weist die gewählte Veröffentlichung, Zustellung und Übermittlung an Wallet-Anbieter an und muss die betroffenen Personen darüber informieren. Empfänger können Daten außerhalb unseres Einflussbereichs speichern oder weitergeben. Bereits importierte Kontakte, heruntergeladene Pässe, Screenshots sowie Kopien in Wallets und bei Empfängern lassen sich durch eine Löschung in unserem System nicht zuverlässig zurückrufen. Wir unterstützen die innerhalb unserer Systeme mögliche Entfernung oder Aktualisierung; eigene Drittanbieterpflichten bleiben unberührt.

Dauer, Rückgabe und Löschung

Die Verarbeitung beginnt erst auf Grundlage eines wirksamen Auftrags einschließlich dieser AVV und dauert, soweit erforderlich, während der beauftragten Nutzung und ihrer Abwicklung an. Die Produktlaufzeit richtet sich nach dem wirksam vereinbarten Hauptvertrag; die AVV schafft keine zusätzliche Hosting- oder Lifetime-Zusage. Bei Beendigung oder entsprechender berechtigter Weisung geben wir die Daten nach Wahl des Verantwortlichen in einem verfügbaren gängigen Format zurück und löschen unsere verbleibenden Kopien oder löschen sie unmittelbar. Die Löschung wird bestätigt. Gesetzlich erforderliche Aufbewahrung und Klausel 10(d) bleiben unberührt; erhaltene Daten werden auf diesen Zweck beschränkt.

Im technischen Regelbetrieb werden Foto-QR-Vorschauen nach höchstens 60 Minuten unzugänglich. Die zugehörige Bereinigung läuft alle 15 Minuten; fehlgeschlagene Löschungen werden erneut versucht. Abgeschlossene technische Hintergrundvorgänge und ihre Versandaufgaben unterliegen regelmäßig der täglichen Bereinigung nach 40 Tagen. Diese Fristen sind keine pauschale Aufbewahrungsberechtigung entgegen einer wirksamen Löschweisung. Aktive Karten und ihre benötigten Bilder werden nicht allein wegen Zeitablaufs entfernt. Für ersetzte Bilder, alte Google-Wallet-Bildvarianten, Zustellereignisse und Wiederherstellungskopien wird im Rahmen einer Löschweisung geprüft, welche Daten noch erforderlich sind und welche entfernt werden müssen.

Eine gesetzliche Aufbewahrung eigener Rechnungs-, Vertrags- oder Nachweisdaten wird getrennt von einer weiteren Nutzung der Mitarbeiter-Karteninhalte behandelt. Soweit eine sofortige Einzelbereinigung von Sicherungskopien technisch nicht möglich ist, bleiben sie gegen reguläre Nutzung gesperrt, werden nach ihrem Löschyklus entfernt und werden bei einer Wiederherstellung erneut von bereits angewiesenen Löschungen bereinigt. Eine unbegrenzte Sicherungskopie wird dadurch nicht gestattet.

Abgrenzung eigener Zwecke und anderer Empfänger

Eigene Nutzerkonten, Geschäftsbeziehungen, Zahlungs- und Steuerabwicklung, Rechtsverteidigung sowie eigene Website-Analyse und Werbung werden, soweit wir dabei selbst Zwecke bestimmen, nach der Datenschutzerklärung und nicht als beliebige Weisung des Firmenkunden verarbeitet. Diese Abgrenzung erlaubt keine Zweckänderung der uns anvertrauten Mitarbeiter-Karteneinhalte. Dodo Payments ist für seine Verkäufer- und Zahlungstätigkeit ein eigenständiger Verantwortlicher. Apple und Google handeln bei ihren eigenen Wallet-, Geräte- und Kontodiensten nach den jeweils einschlägigen Bedingungen; sie werden dadurch nicht pauschal zu Unterauftragsverarbeitern dieses Vertrags. Die von uns angewiesene technische Erstellung und Übermittlung bleibt Teil unserer Leistung. Die gewöhnlichen Mailanbieter der vom Auftraggeber gewählten Empfänger sind keine von uns beauftragten Unterauftragsverarbeiter.

5. Anhang III - Technische und organisatorische Maßnahmen

Die folgenden Maßnahmen beziehen sich auf die in Anhang II beschriebene Verarbeitung. Sie sind von Zertifizierungen und Maßnahmen der Infrastrukturbetreiber zu unterscheiden; wir behaupten keine eigene ISO- oder SOC-Zertifizierung. Maßnahmen dürfen bei mindestens gleichwertigem Schutz fortentwickelt werden. Eine wesentliche Absenkung des Schutzes wird dadurch nicht erlaubt.

Zugang, Berechtigungen und Trennung

Nutzeridentitäten werden über Firebase Authentication geprüft. Serverseitige APIs prüfen den jeweiligen Karteneinhaber, die Gruppen- beziehungsweise Unternehmensberechtigung oder ein zweckgebundenes Zugriffstoken. Administratorzugriff wird gesondert gegen eine aktive Administratorfreigabe geprüft. Zugriff erhalten nur zur Aufgabenerfüllung befugte Personen; diese sind vor Zugriff zur Vertraulichkeit verpflichtet. Berechtigungen sind bei einem Rollenwechsel oder Ausscheiden anzupassen beziehungsweise zu entziehen.

Anonyme Bearbeitungs-, Warenkorb- und Zustellzugriffe verwenden zufällige, zweckgebundene Zugriffsnachweise mit den jeweiligen Laufzeit- und Widerrufsregeln. Soweit der betreffende Mechanismus dies vorsieht, werden nur Hashes der Zugriffstokens gespeichert. Solche Links sind vertraulich zu behandeln. Die öffentlich beabsichtigten Karten- und Downloadadressen sind hiervon zu unterscheiden.

Produktions- und Staging-Datenbanken sowie die zugeordneten Bildspeicher sind logisch getrennt. Serverseitige Datenzugriffe verwenden den jeweils festgelegten Ressourcenkontext. Datenbank- und Storage-Regeln erlauben keinen allgemeinen öffentlichen Zugriff auf private Karten, Vorschau-Schlüssel, Auftrags- oder Workflowdaten. Die bewusst öffentlichen Bild- und Kartenendpunkte prüfen die für ihren jeweiligen Zweck vorgesehenen Voraussetzungen. Der normale Browser erhält keine administrativen Cloud-Zugangsschlüssel.

Übermittlung, Speicherung und Schlüssel

Öffentliche Produktendpunkte verwenden HTTPS. Private Cloud-Storage-Dateien werden über berechtigte Serverzugriffe beziehungsweise zeitlich begrenzte signierte Bildadressen bereitgestellt, soweit sie nicht ausdrücklich zur öffentlichen Kartenausgabe vorgesehen sind. Die verwendeten Google-Cloud-Speicherdienste stellen Verschlüsselung gespeicherter Daten nach ihren Dienstbedingungen bereit. Eine durchgängige Ende-zu-Ende-Verschlüsselung der dauerhaft gespeicherten Karten oder ausschließlich vom Auftraggeber gehaltene Schlüssel sind nicht Bestandteil dieses Dienstes.

Die temporäre Foto-QR-Vorschau verwendet eine gesonderte Bildkopie, einen zufälligen Vorschau-Schlüssel und verschlüsselte Kontaktnutzdaten. Der Server entschlüsselt diese beim Abruf zur vCard-Erzeugung; dies ist keine Verschlüsselung gegenüber unserem Server. Vorschau-Endpunkte sind von unserer anwendungsseitigen Analytics-Verarbeitung ausgenommen. Hosting-Protokollierung ist gesondert auf eine angemessene Minimierung zu prüfen; wir versprechen nicht, dass bei allen Infrastrukturbetreibern keinerlei technische Protokolle entstehen.

Integrität, Betrieb und Wiederherstellung

Gemeinsame Schemas validieren Eingaben und Bildformate. Backend-Berechtigungsprüfungen, transaktionale Zustandsänderungen und wiederholbar ausgeführte Hintergrundaufgaben schützen Kartenänderungen, Zustellung und Löschung vor unzulässigen oder doppelten Verarbeitungsschritten. Hintergrundaufträge besitzen Wiederholungs- und Fehlerzustände; unklare Versandfälle werden nicht blind erneut versendet.

Der Betrieb stützt sich auf verwaltete Cloud-Infrastruktur, deren Verfügbarkeits- und Wiederherstellungsmechanismen sowie dokumentierte Wiederanlauf- und Fehlerbehebungsabläufe. Eine zusätzliche unabhängige Vollsicherung aller Karten, eine bestimmte Sicherungsfrequenz oder eine feste Wiederherstellungszeit wird durch diese AVV nicht als bereits eingerichtet zugesagt. Erforderliche Wiederherstellungsmaßnahmen sind risikogerecht zu prüfen und beim Einsatz zusätzlicher Sicherungen in die Löschprozesse einzubeziehen. Physischer Rechenzentrumszugang und die dortigen Schutzmaßnahmen werden durch die jeweiligen Infrastrukturbetreiber geregelt.

Prüfung, Datenminimierung und Löschung

Änderungen werden versioniert und durch geeignete gezielte Tests geprüft, insbesondere Berechtigungen, Vererbung, Uploads, Löschung und Versandwiederholungen. Der Schutzbedarf, Berechtigungen, Dienstleister und die Wirksamkeit der Maßnahmen sind regelmäßig sowie nach erheblichen Änderungen oder Vorfällen zu überprüfen. Betriebssysteme, Laufzeitumgebungen und Abhängigkeiten sind entsprechend dem Risiko zu pflegen. Kundeninhalte sollen für Tests nur verwendet werden, soweit dies erforderlich, autorisiert und durch dieselben Schutzpflichten gedeckt ist; synthetische Daten sind vorzuziehen.

Browserlokale anonyme Warenkörbe enthalten überwiegend Referenzen und Zugriffsnachweise statt vollständiger Karteninhalte. Die reine Online-Visitenkarte und Foto-Download-Flächen laden keine anwendungsseitigen Werbe- oder Analytics-Skripte. Löschaufträge berücksichtigen abhängige Kartenbilder, Pässe und Referenzen. Technische Bereinigungen und fehlgeschlagene Löschungen werden über die vorhandenen Hintergrundabläufe abgearbeitet. Betriebsprotokolle und Supportnachrichten sind auf notwendige Angaben zu begrenzen; vollständige Mitarbeiterlisten oder Bildkopien gehören nicht ohne Bedarf in eine Supportnachricht.

Unterstützung, Vorfälle und Nachweise

Der Datenschutzkontakt in Anhang I nimmt Weisungen und Betroffenenanfragen entgegen. Wir prüfen die Zuordnung und Berechtigung, leiten Anfragen erforderlichenfalls an den Verantwortlichen weiter und unterstützen innerhalb unseres Einflussbereichs bei Auskunft, Berichtigung, Export, Einschränkung und Löschung. Für Sicherheitsbewertungen und erforderliche Datenschutz-Folgenabschätzungen stellen wir die verfügbaren Informationen zu Verarbeitung und Schutzmaßnahmen bereit. Behördliche Meldungen und die Kommunikation mit betroffenen Personen richten sich nach der gesetzlich vorgesehenen Rollenverteilung.

Datenschutzverletzungen werden nach Bekanntwerden unverzüglich an den Verantwortlichen gemeldet; unvollständige Informationen werden schrittweise ergänzt. Mitgeteilt werden, soweit bekannt, Art und Zeitpunkt, betroffene Daten und Personengruppen, geschätzter Umfang, wahrscheinliche Folgen, Kontaktstelle sowie ergriffene oder geplante Gegenmaßnahmen. Relevante Nachweise werden gesichert, Abhilfe und weitere Abstimmung dokumentiert. Die gesetzliche Meldefrist des Verantwortlichen wird dadurch nicht auf uns verschoben oder verlängert.

Nachweise und Prüfungen erfolgen zunächst anhand geeigneter Unterlagen und, soweit nötig, durch die in Klausel 7.6 vorgesehenen Audits. Schutz anderer Kunden, Geschäftsgeheimnisse und Betriebssicherheit sind angemessen zu berücksichtigen, ohne die vereinbarten oder gesetzlichen Kontrollrechte auszuschließen. Zugriff auf Dienstleisterunterlagen und erforderliche weitere Nachweise wird im Rahmen der verfügbaren vertraglichen Rechte unterstützt.

6. Anhang IV - Dienstleister, Unterauftragsverarbeitung und Übermittlungen

Allgemeine Genehmigung und Änderungen

Für die in diesem Anhang beschriebenen Verarbeitungsteile gilt bei Vertragsabschluss die allgemeine schriftliche Genehmigung nach Klausel 7.7(a), Option 2. Erfasst sind nur tatsächlich eingesetzte Dienste und die darin benötigten Daten. Vor einer Hinzunahme oder Ersetzung informieren wir den Verantwortlichen ausdrücklich in Textform mindestens 30 Tage im Voraus über Anbieter, Tätigkeit, Ort und relevante Garantien. Ein bloßes stilles Aktualisieren dieser Webseite ersetzt die Mitteilung nicht. Einwendungen werden vor dem Einsatz geprüft; lässt sich ein berechtigter Datenschutz-Einwand nicht ausräumen, wird die betroffene Verarbeitung nicht ohne tragfähige Lösung fortgeführt.

Google Cloud und Firebase

Anbieter sind die für die beauftragten Dienste vertraglich zuständigen Google-Einheiten, insbesondere Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland, sowie für einschlägige Firebase- und Infrastrukturleistungen Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, und Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Die Zuordnung richtet sich nach dem bestehenden Vertrag und der [Google-Vertragspartnerübersicht](#). Die konkret beauftragte Einheit und Vertragsgrundlage sind im Dienstleister-Nachweis zu dokumentieren und dem Verantwortlichen auf Anfrage zugänglich zu machen.

Verarbeitet werden Kartendaten, Bilder, Passdateien, Berechtigungszuordnungen, Zustell- und Workflowdaten sowie erforderliche technische Metadaten für Datenbank, Cloud Storage, Backend, Authentifizierung und Hintergrundaufgaben. Die Backend- und Aufgabenregion ist im Produkt auf europe-west1 ausgerichtet. Dies ist keine Zusage, dass sämtliche Datenbanken, Speicher, Authentifizierungs-, Support- und Metadaten ausschließlich in dieser Region oder im EWR verarbeitet werden.

Maßgeblich sind die anwendbaren [Firebase Data Processing and Security Terms](#), das [Google Cloud Data Processing Addendum](#), die tatsächlich vereinbarten Ressourcenstandorte und die jeweils einschlägigen [Firebase-Unterauftragsverarbeiter](#) beziehungsweise [Google-Cloud-Unterauftragsverarbeiter](#). Angaben zu konkreten Einheiten, Tätigkeiten und Ländern in diesen Listen sind für die genutzten Dienste zu berücksichtigen; nicht jeder dort gelistete Dienst wird von uns genutzt.

Vercel

Vercel Inc., 440 N Barranca Avenue #4133, Covina, CA 91723, USA, betreibt die produktive Webanwendung und deren Auslieferungsinfrastruktur. Je nach Route werden Kartendarstellung, Bilder oder Downloads sowie Anfragedaten wie IP-Adresse, Browserinformationen und Referenzen durch diese Infrastruktur übertragen oder verarbeitet. Dies ist von Vercel Flags für eigene Produktexperimente zu unterscheiden.

Wir nutzen Vercel Pro mit der dafür vereinbarten [Vercel-DPA](#). Verarbeitung kann in den USA und weiteren Standorten des Auslieferungsnetzes und der für die gewählten Dienste eingesetzten [Unterauftragsverarbeiter](#) stattfinden. Eine ausschließlich europäische Verarbeitung wird nicht vereinbart.

Transaktionale E-Mails über Resend

Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA, stellt angeforderte Karten- und andere auftragsbezogene E-Mails zu. Verarbeitet werden die benötigten Empfängeradressen, gegebenenfalls Namen, Nachrichteninhalte, Zustelllinks und Zustellmetadaten. Dies umfasst nur die tatsächlich beauftragte Zustellung, nicht eine allgemeine Freigabe der Mitarbeiterdaten für Newsletter oder Werbung.

Resend beschreibt primäre Verarbeitung in den USA. Grundlage sind die [Resend-DPA](#) und die für das Konto vereinbarten Übermittlungsgarantien. Weitere eingesetzte Anbieter ergeben sich aus der [Resend-Unterauftragsverarbeiterliste](#); für Hosting und Zustellung nennt Resend insbesondere Amazon Web Services. Die gesamte Liste bedeutet nicht, dass jede dort genannte Funktion unsere Kartendaten erhält.

Drittlandschutz, weitere Empfänger und Nachweise

Bei Übermittlungen außerhalb des EWR müssen die Voraussetzungen des Kapitels V DSGVO tatsächlich erfüllt sein. Je nach Empfänger und Verarbeitung kommen ein wirksamer Angemessenheitsbeschluss innerhalb seines Anwendungsbereichs oder die anwendbaren Übermittlungsklauseln des Beschlusses (EU) 2021/914 mit erforderlicher Bewertung und ergänzenden Maßnahmen in Betracht. Die Klauseln dieses Vertrags nach 2021/915 ersetzen diese Übermittlungsgrundlage nicht. Der Auftragsverarbeiter prüft und dokumentiert die passende Grundlage; eine bloße Anbieterliste oder ein allgemeines DPF- beziehungsweise SCC-Versprechen genügt dafür nicht.

Mit Unterauftragsverarbeitern werden die nach Klausel 7.7 erforderlichen Pflichten vereinbart. Weitere Unterauftragnehmerketten, Änderungen, Nachweise und Anfragen werden nach dieser Klausel behandelt. Dem Verantwortlichen werden auf Anfrage die einschlägigen Anbieteridentitäten, Verarbeitungsorte und Schutzgrundlagen sowie die nach Klausel 7.7(c) verfügbaren Vertragskopien bereitgestellt. Anbieter-Webseiten dienen als Informationsquellen und ändern die vereinbarte Vertragsfassung nicht automatisch.

Apple Wallet, die eigenständigen Google-Wallet-Kontodienste, Google Maps/Places bei angeforderter Standortsuche, vom Auftraggeber gewählte Linkziele und Empfänger-Mailanbieter sind entsprechend der Rollenabgrenzung in Anhang II andere Empfänger. Sie werden durch diese Liste nicht zu pauschal weisungsgebundenen Unterauftragsverarbeitern erklärt. Eigene Analyse-, Werbe-, Zahlungs- und KI-Dienste werden nicht als Teil der Verarbeitung von Mitarbeiter-Karteninhalten genehmigt. Falls für einen gesonderten Auftrag weitere Dienstleister benötigt werden, sind sie vor ihrem Einsatz nach den vorstehenden Regeln einzubeziehen.