

Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 25. Juli 2026 · Version 2026-07-25

Zwischen

Verantwortlicher

Die Angaben des Verantwortlichen (Name beziehungsweise Firma, Anschrift, gesetzliche Vertretung, gegebenenfalls Register- und Umsatzsteuerangaben) ergeben sich aus den Angaben bei der elektronischen Annahme dieses Vertrages auf fahrpilot.pro/rechtliches/avv. Sie werden in der Annahme-Bestätigung dokumentiert. Ein manuelles Ausfüllen dieses Feldes ist nicht erforderlich.

— nachfolgend „Verantwortlicher“ oder „Fahrschule“ genannt —

und

Auftragsverarbeiter

Jan Kotthoff
Einzelunternehmen
Brühlstraße 8A
65191 Wiesbaden
Deutschland
E-Mail: kontakt@fahrpilot.pro

— nachfolgend „Auftragsverarbeiter“ oder „FahrPilot“ genannt —

— gemeinsam „die Parteien“ genannt —

Präambel

Der Verantwortliche nutzt die vom Auftragsverarbeiter betriebene Software-as-a-Service-Plattform „FahrPilot“ (nachfolgend „Plattform“) auf Grundlage der zwischen den Parteien geschlossenen Nutzungsvereinbarung einschließlich der Allgemeinen Geschäftsbedingungen (nachfolgend „Hauptvertrag“). Im Rahmen dieser Nutzung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO.

§ 1 Gegenstand und Dauer

(1) Gegenstand des Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen zur Erbringung der im Hauptvertrag vereinbarten Leistungen (Betrieb einer Online-Plattform für die Verwaltung von Fahrschulen: Terminplanung, Theorie- und Praxisausbildung, Schüler- und Prüfungsverwaltung sowie zugehörige Benachrichtigungen).

(2) Die Dauer dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Der Vertrag endet automatisch mit Beendigung des Hauptvertrages, ohne dass es einer gesonderten Kündigung bedarf.

§ 2 Art und Zweck der Verarbeitung, Datenkategorien und betroffene Personen

(1) Art und Zweck der Verarbeitung sowie die Kategorien der personenbezogenen Daten und der betroffenen Personen ergeben sich aus Anhang 1 zu diesem Vertrag.

(2) Der Auftragsverarbeiter darf die überlassenen Daten ausschließlich zu den in Anhang 1 festgelegten Zwecken verarbeiten.

§ 3 Rechte und Weisungen des Verantwortlichen

(1) Der Verantwortliche bleibt allein Herr der Daten im Sinne der DSGVO. Er ist berechtigt, dem Auftragsverarbeiter jederzeit ergänzende Weisungen zu Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen können in Textform (z. B. per E-Mail) erfolgen und werden vom Auftragsverarbeiter dokumentiert.

(2) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Der Hauptvertrag und dieser Vertrag gelten als solche dokumentierte Weisung.

(3) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Ausführung der betreffenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

§ 4 Pflichten des Auftragsverarbeiters

(1) Vertraulichkeit. Der Auftragsverarbeiter verpflichtet alle Personen, die zur Verarbeitung der Daten befugt sind, schriftlich zur Vertraulichkeit oder stellt sicher, dass diese einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung des Vertrages fort.

(2) Technische und organisatorische Maßnahmen. Der Auftragsverarbeiter trifft die in Art. 32 DSGVO geforderten technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus. Die konkret umgesetzten Maßnahmen ergeben sich aus Anhang 2. Der Auftragsverarbeiter darf die Maßnahmen im Laufe der Zeit weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Unterstützung bei Betroffenenrechten. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten zur Beantwortung von Anträgen betroffener Personen nach Art. 12 bis 22 DSGVO (insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch). Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter.

(4) Unterstützung bei sonstigen Pflichten. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung und Benachrichtigung bei Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(5) Meldung von Verletzungen des Schutzes personenbezogener Daten. Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm nachweislich bekannt gewordene, hinreichend belegte Verletzung des Schutzes personenbezogener Daten, die im Rahmen der auftragsgemäßen Verarbeitung erfolgt und die Daten des Verantwortlichen konkret betrifft, in Textform. Die Meldung erfolgt so bald wie unter den Umständen zumutbar, spätestens innerhalb von 72 Stunden nach eigener bestätigter Kenntnisnahme. Die Meldung enthält die in Art. 33 Abs. 3 DSGVO genannten Angaben in dem Umfang, in dem sie dem Auftragsverarbeiter zum Zeitpunkt der Meldung bekannt sind; ergänzende Informationen werden nachgereicht, sobald sie verfügbar sind. Verletzungen im Verantwortungsbereich der Unter-Auftragsverarbeiter werden gegenüber dem Verantwortlichen weitergegeben, sobald der Auftragsverarbeiter von diesen selbst informiert wurde; eine eigene Ermittlungspflicht des Auftragsverarbeiters bei Unter-Auftragsverarbeitern besteht nicht.

(6) Löschung und Rückgabe nach Vertragsende. Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter alle in seinem Auftrag verarbeiteten personenbezogenen Daten oder gibt sie nach Wahl des Verantwortlichen zurück, sofern und soweit nicht eine gesetzliche Aufbewahrungspflicht (insbesondere nach § 257 HGB, § 147 AO) einer Löschung entgegensteht. Für die Dauer solcher Aufbewahrungspflichten wird die Verarbeitung eingeschränkt. Vor der Löschung räumt der Auftragsverarbeiter dem Verantwortlichen eine Frist von 30 Kalendertagen zur eigenständigen Datensicherung ein; der Hauptvertrag sieht hierfür einen Export in einem gängigen, maschinenlesbaren Format vor. Die Frist beginnt mit dem Wirksamwerden der Vertragsbeendigung. Wünscht der Verantwortliche eine darüber hinausgehende Datenrückgabe (z. B. individuelle Export-Formate), trägt er den hierdurch entstehenden angemessenen

nen Aufwand. Sicherungskopien werden durch die reguläre Rotation überschrieben; eine sofortige, außerplanmäßige Löschung einzelner Sicherungskopien ist ausgeschlossen. Der Auftragsverarbeiter bestätigt die erfolgte Löschung auf Verlangen in Textform.

§ 5 Unter-Auftragsverarbeiter

(1) Der Auftragsverarbeiter darf zur Erfüllung seiner Leistungen weitere Auftragsverarbeiter („Unter-Auftragsverarbeiter“) einsetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unter-Auftragsverarbeiter sind in Anhang 3 aufgeführt. Der Verantwortliche stimmt dem Einsatz dieser Unter-Auftragsverarbeiter mit Abschluss dieses Vertrages zu.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder den Austausch von Unter-Auftragsverarbeitern mindestens 30 Kalendertage im Voraus in Textform (z. B. per E-Mail an die im Konto hinterlegte Adresse oder durch Benachrichtigung in der Plattform). Der Verantwortliche kann einem Wechsel innerhalb dieser Frist aus wichtigem, datenschutzrechtlich begründetem Grund widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt.

(3) Im Fall eines berechtigten Widerspruchs sind die Parteien verpflichtet, eine einvernehmliche Lösung zu suchen. Kommt eine solche nicht zustande, steht dem Verantwortlichen ein außerordentliches Kündigungsrecht des Hauptvertrages zu.

(4) Der Auftragsverarbeiter bindet die eingesetzten Unter-Auftragsverarbeiter datenschutzrechtlich nach Maßgabe von Art. 28 Abs. 4 DSGVO. Dies erfolgt nach Wahl des Auftragsverarbeiters durch (a) Abschluss eines individuellen Auftragsverarbeitungsvertrages, (b) Zugrundelegung der vom jeweiligen Unter-Auftragsverarbeiter angebotenen Standard-Datenschutzbedingungen, sofern diese den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechen, oder (c) Zugrundelegung von Standardvertragsklauseln der Europäischen Kommission bei Drittlandtransfers. Der Auftragsverarbeiter wählt Unter-Auftragsverarbeiter aus, die hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen bieten.

§ 6 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, sich vom Auftragsverarbeiter die Einhaltung der Pflichten aus diesem Vertrag nachweisen zu lassen. Der Auftragsverarbeiter stellt hierfür alle erforderlichen Informationen bereit.

(2) Der Nachweis erfolgt in der Regel durch:

- Selbstauskunft des Auftragsverarbeiters in Textform,
- die Dokumentation der umgesetzten technischen und organisatorischen Maßnahmen (Anhang 2),
- die Liste der eingesetzten Unter-Auftragsverarbeiter (Anhang 3),
- öffentlich verfügbare Testate, Zertifikate oder Prüfberichte der Unter-Auftragsverarbeiter, soweit vorhanden.

(3) Die vertraglichen Vereinbarungen des Auftragsverarbeiters mit seinen Unter-Auftragsverarbeitern — einschließlich ihres Wortlauts und aller Vertragsauszüge — sind Geschäftsgeheimnisse im Sinne des GeschGehG und werden dem Verantwortlichen nicht offengelegt. Die vertragliche Zusicherung des Auftragsverarbeiters nach § 5 Abs. 4 sowie die Angaben in Anhang 3 gelten als hinreichende Information im Sinne von Art. 28 Abs. 3 lit. h DSGVO.

(4) Reichen die Nachweise nach Absatz 2 im Einzelfall nicht aus, kann der Verantwortliche ergänzende Auskünfte in Textform verlangen. Der Auftragsverarbeiter beantwortet berechnigte, schriftliche Fragen zur Einhaltung dieses Vertrages innerhalb von 30 Kalendertagen. Der Auftragsverarbeiter betreibt keine eigene physische IT-Infrastruktur; sämtliche Datenverarbeitung findet ausschließlich bei den in Anhang 3 aufgeführten Unter-Auftragsverarbeitern statt. Vor-Ort-Kontrollen sind daher nicht Gegenstand der ordentlichen Überprüfung und nur bei konkreten, dokumentierten Anhaltspunkten für einen wesentlichen Datenschutzverstoß gegen den Auftragsverarbeiter selbst zulässig; sie bedürfen einer gesonderten Vereinbarung in Textform. Überprüfungen bei Unter-Auftragsverarbeitern sind ausgeschlossen; diese liegen in der Verantwortung des Auftragsverarbeiters. Ordentliche Auskunftsverlangen sind auf einmal pro Kalen-

derjahr beschränkt. Sämtliche Kosten der Überprüfung einschließlich eines angemessenen Aufwandsersatzes des Auftragsverarbeiters trägt der Verantwortliche.

§ 7 Datenübermittlung in Drittländer

(1) Eine Übermittlung personenbezogener Daten in Drittländer außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Rechtsgrundlage der Übermittlung ist eine oder mehrere der folgenden Alternativen, jeweils ergänzt um die nach der Rechtsprechung erforderlichen zusätzlichen Maßnahmen:

- ein Angemessenheitsbeschluss der Europäischen Kommission (insbesondere EU-US Data Privacy Framework für zertifizierte US-Unternehmen),
- Standardvertragsklauseln der Europäischen Kommission gemäß Durchführungsbeschluss (EU) 2021/914,
- die Zustimmung des Verantwortlichen zu den Standard-Datenschutzbedingungen des jeweiligen Unter-Auftragsverarbeiters, die die vorgenannten Rechtsgrundlagen umsetzen.

(3) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unter-Auftragsverarbeiter verarbeiten die Daten in Rechenzentren innerhalb der EU (Anhang 3). Mit Annahme dieses Vertrages stimmt der Verantwortliche etwaigen dort aufgeführten Drittlandbezügen zu.

(4) Sollte ein Angemessenheitsbeschluss nach Vertragsschluss aufgehoben oder für unwirksam erklärt werden, greifen für die betroffenen Übermittlungen unmittelbar die Standardvertragsklauseln als Rechtsgrundlage, sofern der jeweilige Unter-Auftragsverarbeiter diese anbietet. Der Auftragsverarbeiter informiert den Verantwortlichen über solche Änderungen; ein Widerspruchsrecht besteht nach § 5 Abs. 2 und 3.

§ 8 Haftung

(1) Für die Haftung gegenüber betroffenen Personen aus der Verletzung von Datenschutzvorschriften gelten die Regelungen des Art. 82 DSGVO.

(2) Im Innenverhältnis zwischen den Parteien haftet der Auftragsverarbeiter dem Verantwortlichen für Schäden aus der Verletzung dieses Vertrages nach den folgenden Grundsätzen: (a) unbeschränkt für Vorsatz und grobe Fahrlässigkeit, für die Verletzung von Leben, Körper oder Gesundheit sowie in sonstigen Fällen zwingender gesetzlicher Haftung; (b) für die Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) bei leichter Fahrlässigkeit beschränkt auf den vertragstypisch vorhersehbaren Schaden; (c) im Übrigen ist die Haftung ausgeschlossen.

(3) Die Haftungsbeschränkung gilt für alle Ansprüche unabhängig vom Rechtsgrund, insbesondere aus unerlaubter Handlung. Sie gilt nicht für Ansprüche des Verantwortlichen nach dem Produkthaftungsgesetz oder für die Verletzung ausdrücklich übernommener Garantien.

(4) Werden gegen eine Partei Ansprüche einer betroffenen Person geltend gemacht, informiert diese die andere Partei unverzüglich, damit eine gemeinsame Verteidigung koordiniert werden kann. Ein Vergleich oder Anerkenntnis darf nur nach vorheriger Abstimmung mit der jeweils anderen Partei geschlossen werden.

(5) Regressansprüche zwischen den Parteien nach Art. 82 Abs. 5 DSGVO richten sich nach dem tatsächlichen Verantwortungsbeitrag der Parteien; im Verhältnis zwischen den Parteien wird vermutet, dass die Verantwortungsanteile den in Art. 4 Nr. 7 und 8 DSGVO festgelegten Rollen entsprechen (der Verantwortliche bestimmt Zweck und Mittel, der Auftragsverarbeiter verarbeitet weisungsgebunden).

§ 9 Höhere Gewalt

(1) Ereignisse höherer Gewalt oder vergleichbare, außerhalb der Sphäre des Auftragsverarbeiters liegende Störungen (insbesondere Ausfälle bei Unter-Auftragsverarbeitern, großflächige Netz- oder Internet-Störungen, Cyber-Angriffe auf die Infrastruktur eines Unter-Auftragsverarbeiters trotz angemessener Schutzmaßnahmen, hoheitliche Maßnahmen,

Pandemien) befreien den Auftragsverarbeiter für die Dauer der Störung von den betroffenen Leistungspflichten. Fristen aus diesem Vertrag verlängern sich entsprechend.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über solche Ereignisse und die voraussichtliche Dauer der Beeinträchtigung.

§ 10 Verjährung

Ansprüche des Verantwortlichen gegen den Auftragsverarbeiter aus oder im Zusammenhang mit diesem Vertrag verjähren, soweit gesetzlich zulässig, in zwölf Monaten ab Kenntnis des Verantwortlichen von den anspruchsbegründenden Umständen und der Person des Anspruchsgegners, spätestens jedoch drei Jahre nach Entstehung des Anspruchs. Gesetzliche Ausnahmen (insbesondere für Vorsatz und die Verletzung von Leben, Körper und Gesundheit) bleiben unberührt.

§ 11 Änderungsvorbehalt für Anhänge

(1) Der Auftragsverarbeiter ist berechtigt, die Anhänge 2 (technische und organisatorische Maßnahmen) und 3 (Unter-Auftragsverarbeiter) einseitig zu aktualisieren, sofern und soweit hierdurch das vertraglich vereinbarte Schutzniveau nicht wesentlich verringert wird und die Aktualisierung durch technische, wirtschaftliche oder rechtliche Entwicklungen sachlich gerechtfertigt ist.

(2) Wesentliche Änderungen (insbesondere Wechsel oder Hinzuziehung von Unter-Auftragsverarbeitern) werden dem Verantwortlichen nach § 5 Abs. 2 mitgeteilt; das dort geregelte Widerspruchsrecht bleibt unberührt. Nicht wesentliche Aktualisierungen (etwa redaktionelle Präzisierungen ohne Absenkung des Schutzniveaus) werden auf der Plattform dokumentiert.

§ 12 Vertragsdauer und Beendigung

(1) Der Vertrag beginnt mit seiner Annahme durch den Verantwortlichen und läuft für die Dauer des Hauptvertrages.

(2) Der Vertrag endet automatisch mit Beendigung des Hauptvertrages, unabhängig vom Grund der Beendigung.

(3) Nach Beendigung gelten die Pflichten aus § 4 Abs. 6 (Löschung/Rückgabe) sowie § 4 Abs. 1 (Vertraulichkeit) fort.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Dies gilt auch für die Abbedingung dieses Textformerfordernisses. Der Änderungsvorbehalt nach § 11 für die Anhänge 2 und 3 bleibt hiervon unberührt.

(2) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, berührt dies nicht die Wirksamkeit der übrigen Bestimmungen. Die Parteien werden die unwirksame Bestimmung durch eine wirksame Bestimmung ersetzen, die dem beabsichtigten wirtschaftlichen und rechtlichen Zweck möglichst nahekommt.

(3) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(4) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.

(5) Im Fall von Widersprüchen zwischen den Regelungen dieses Vertrages und den Regelungen des Hauptvertrages gehen die Regelungen dieses Vertrages vor, soweit sie den Datenschutz betreffen.

Annahme des Vertrages

Verantwortlicher

Die Annahme dieses Vertrages erfolgt durch den Verantwortlichen elektronisch durch Klick auf „Annahme bestätigen“

auf fahrpilot.pro/rechtliches/avv (Anmeldung mit einem FahrPilot-Konto erforderlich). Diese Form genügt der Textform gemäß § 126b BGB und begründet einen wirksamen Vertragsschluss. Alternativ ist eine formlose Bestätigung per E-Mail an kontakt@fahrpilot.pro mit dem Wortlaut „AVV in der Fassung vom 25. Juli 2026 akzeptiert“ ausreichend.

Die elektronische Annahme wird vom Auftragsverarbeiter unter Angabe von Zeitstempel, annehmender Nutzer-Kennung, Fahrschul-Zuordnung und akzeptierter Vertragsversion dokumentiert. Der Verantwortliche erhält eine Bestätigungs-E-Mail mit seinen bei der Annahme gemachten Firmendaten und dem Annahmezeitpunkt als Nachweis für seine Unterlagen.

Auftragsverarbeiter

Jan Kotthoff, Einzelunternehmen
Wiesbaden, den 25. Juli 2026

(Elektronische Erklärung — kein handschriftliches Zeichen erforderlich, § 126b BGB)

Anhang 1 — Art, Zweck, Datenkategorien und betroffene Personen

1. Zweck der Verarbeitung

Betrieb einer Online-Plattform für die Verwaltung von Fahrschulen, einschließlich:

- Anlage und Verwaltung von Fahrschülern, Ausbildungen und Nachweis-Status
- Terminplanung: Fahrstunden, Theorieunterricht, Arbeitszeiten und Abwesenheiten
- Selbstbuchung von Fahrstunden und Theorieterminen durch Fahrschüler
- Anwesenheits- und Fortschrittsverwaltung (Pflichtstunden, Sonderfahrten)
- Prüfungsverwaltung
- Einbindung gesetzlicher Vertreter (Minderjährige, begleitetes Fahren ab 17)
- Termin-Erinnerungen, Bestätigungen und sonstige transaktionale Kommunikation
- Fehleranalyse und Sicherstellung des Plattformbetriebs

Optionales Zahlungsmodul: Die Plattform ermöglicht dem Verantwortlichen, Karten- und SEPA-Zahlungen seiner Fahrschüler über sein EIGENES Stripe-Konto abzuwickeln. Karten- und Kontodaten der Zahlenden werden ausschließlich von Stripe erhoben und verarbeitet; sie werden dem Auftragsverarbeiter weder übermittelt noch sind sie ihm zugänglich. Der Auftragsverarbeiter verarbeitet insoweit ausschließlich Zahlungs-Metadaten (Zahlungsstatus, Beträge, SEPA-Mandatsreferenz, Stripe-Kennungen, Zeitpunkt der Vorabankündigung). Der Verantwortliche schließt mit Stripe einen eigenen Vertrag (siehe AGB § 11a).

2. Art der Verarbeitung

Erheben, Speichern, Auslesen, Anzeigen, Verwenden, Übermitteln (an vom Verantwortlichen berechnigte Empfänger und an Unter-Auftragsverarbeiter gemäß Anhang 3), Sichern (Backups), Wiederherstellen, Löschen.

3. Kategorien personenbezogener Daten

Kategorie	Beispiele
Stammdaten der Fahrschüler	Name, Anschrift, Geburtsdatum, Geburtsort, Geburtsname, Staatsangehörigkeit, Kundennummer
Daten gesetzlicher Vertreter	Name, Anschrift, Kontaktdaten, Verbindung zur Fahrschülerin oder zum Fahrschüler, Zeitpunkt erteilter Einwilligungen

Konto- und Zugangsdaten	Benutzer-Kennung, E-Mail-Adresse, Anmeldezeitpunkte — Passwörter ausschließlich als kryptographischer Hash beim Anmeldedienst, nie in der Plattform-Datenbank
Ausbildungsdaten	Führerscheinklasse, Ausbildungsart, Getriebeart, Ausbildungsfortschritt, Freischaltungen, Status der vorzulegenden Nachweise
Termin- und Anwesenheitsdaten	Gebuchte und wahrgenommene Fahrstunden und Theorieeinheiten, Absagen, Anwesenheiten
Prüfungsdaten	Anmeldungen, Termine, Ergebnisse
Zahlungs-Metadaten (optionales Zahlungsmodul)	Zahlungsstatus, Beträge, SEPA-Mandatsreferenz, Stripe-Kennungen (Kunde/Konto), Zeitpunkt der Vorabankündigung — KEINE Karten- oder Kontodaten
Kommunikationsdaten	Versendete transaktionale E-Mails und deren Versandprotokoll
Mitarbeiterdaten des Verantwortlichen	Name, E-Mail-Adresse, Rolle und Berechtigungen von Fahrlehrern und Verwaltungspersonal
Technische Daten	IP-Adressen, Geräte- und Browserdaten, Zeitstempel — soweit zur Sicherstellung des Betriebs erforderlich

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. Nachweise wie der Sehtest werden ausschließlich als Status („liegt vor“ / „liegt nicht vor“) geführt — ohne Befunde, ohne Diagnosen, ohne hochgeladene Dokumente.

4. Kategorien betroffener Personen

- Fahrschülerinnen und Fahrschüler des Verantwortlichen, einschließlich Minderjähriger
- gesetzliche Vertreter und Begleitpersonen
- Mitarbeiterinnen und Mitarbeiter des Verantwortlichen (Fahrlehrer, Büro)
- Interessentinnen und Interessenten, die über die Plattform Kontakt aufnehmen

Anhang 2 — Technische und organisatorische Maßnahmen (TOM)

Gemäß Art. 32 DSGVO trifft der Auftragsverarbeiter die folgenden technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus.

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

1.1 Zutrittskontrolle: Kein physischer Serverbetrieb durch den Auftragsverarbeiter. Alle Datenverarbeitungssysteme werden bei zertifizierten Unter-Auftragsverarbeitern in EU-Rechenzentren betrieben (Anhang 3). Diese verfügen über eigene Zutrittskontrollen.

1.2 Zugangskontrolle:

- Zugriff ausschließlich über verschlüsselte Verbindungen (TLS)
- Persönliche, individuelle Zugangsdaten für jede Person mit Systemzugriff
- Zwei-Faktor-Authentifizierung für die administrativen Zugänge zur Infrastruktur (Hosting, Datenbank, Quellcode, E-Mail-Versand)
- Passwörter der Plattform-Nutzer ausschließlich als kryptographischer Hash beim Anmeldedienst — die Plattform-Datenbank speichert keine Passwörter

- Verschlüsselung ruhender Daten (AES-256 oder gleichwertig) bei den Hosting-Unter-Auftragsverarbeitern

1.3 Zugriffskontrolle:

- Rollenbasierte Berechtigungen: Inhaber, Büro, Fahrlehrer, Fahrschüler und gesetzliche Vertreter sehen jeweils nur den für ihre Rolle bestimmten Bereich
- Mandantentrennung auf Anwendungsebene: Jede Datenbankabfrage ist an die Fahrschule der angemeldeten Sitzung gebunden; ein Zugriff auf Daten einer anderen Fahrschule ist ausgeschlossen und wird durch automatisierte Tests laufend geprüft
- Fahrlehrer sehen nur die ihnen zugewiesenen Fahrschüler

1.4 Support-Zugriff des Auftragsverarbeiters:

- Beginn, Ende und jede einzelne Änderung eines Support-Zugriffs werden protokolliert — mit Zeitpunkt, handelnder Person und betroffener Fahrschule
- Das Protokoll ist durch einen Mechanismus der Datenbank selbst gegen Änderung und Löschung geschützt — auch gegenüber dem Auftragsverarbeiter
- Während des Zugriffs erscheint in der Software durchgehend ein sichtbarer Hinweis
- Die Support-Sitzung endet automatisch spätestens nach vier Stunden

1.5 Pseudonymisierung: Interne Kennungen (UUIDs) statt sprechender Kennzeichen.

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

- Verschlüsselte Übertragung sämtlicher Daten zwischen Endgerät, Anwendung, Datenbank und E-Mail-Versand
- Protokollierung sicherheitsrelevanter Änderungen
- Datenintegrität durch Regeln in der Datenbank selbst (unter anderem Ausschluss-Regeln gegen Doppelbelegungen)
- Versionierung aller Software-Änderungen (Git)

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

- Betrieb auf redundanter Cloud-Infrastruktur in EU-Rechenzentren
- Automatische tägliche Datenbank-Sicherungen, Aufbewahrung mindestens 7 Tage, verschlüsselt gespeichert
- Überwachung der Systemverfügbarkeit durch die Infrastruktur-Anbieter

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

- Automatisierte Prüfungen vor jeder Veröffentlichung: Typprüfung, statische Analyse und End-to-End-Tests — darunter Tests, die die Mandantentrennung und die Zugriffsrechte jeder Rolle ausdrücklich prüfen
- Fortlaufende Sicherheits-Aktualisierung der eingesetzten Systeme und Bibliotheken
- Dokumentation der Verarbeitungstätigkeiten
- Sicherheitsvorfälle werden dokumentiert und ausgewertet

5. Auftragskontrolle (Art. 28 DSGVO)

- Bindung aller Unter-Auftragsverarbeiter über deren Standard-Datenschutzbedingungen, die den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechen
- Prüfung der Datenschutz-Dokumentation der Unter-Auftragsverarbeiter vor Beauftragung

6. Datenschutzbeauftragter

Der Auftragsverarbeiter ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet (Art. 37 DSGVO, § 38 BDSG): Es sind nicht mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung befasst, und die

Kerntätigkeit besteht weder in umfangreicher systematischer Überwachung noch in umfangreicher Verarbeitung besonderer Datenkategorien. Datenschutzanfragen sind an kontakt@fahrpilot.pro zu richten.

Anhang 3 — Liste der Unter-Auftragsverarbeiter

Der Auftragsverarbeiter setzt zum Zeitpunkt des Vertragsschlusses die folgenden Unter-Auftragsverarbeiter ein. Die Bindung erfolgt gemäß § 5 Abs. 4 dieses Vertrages.

Unter-Auftragsverarbeiter	Sitz	Ort der Verarbeitung	Leistung	Bindung / Rechtsgrundlage
Vercel Inc.	Walnut, CA, USA	EU (Frankfurt, fra1) für die Ausführung der Anwendung; Auslieferung statischer, nicht personenbezogener Inhalte über ein weltweites Content-Delivery-Netz	Hosting und Ausführung der Web-Anwendung	Standard-DPA des Anbieters, EU-Region konfiguriert; EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln
Supabase Inc.	Wilmington, DE, USA	EU (Frankfurt am Main, eu-central-1)	Datenbank (PostgreSQL) und Anmeldeverfahren	Standard-DPA des Anbieters; EU-Verarbeitung; ergänzend Standardvertragsklauseln
Resend (Plus Five Five, Inc.)	San Francisco, CA, USA	EU (Irland, eu-west-1)	Versand transaktionaler E-Mails	Standard-DPA des Anbieters; EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln
Stripe Payments Europe, Ltd.	Dublin, Irland	EU (Irland)	Optionales Zahlungsmodul: Zahlungsabwicklung über das eigene Stripe-Konto des Verantwortlichen; verarbeitet Karten-/Kontodaten der Zahlenden (dem Auftragsverarbeiter nicht zugänglich)	Eigener Vertrag des Verantwortlichen mit Stripe (siehe AGB § 11a); Stripe-DPA; EU-Verarbeitung

Änderungen dieser Liste werden dem Verantwortlichen gemäß § 5 Abs. 2 dieses Vertrages mitgeteilt. Die aktuell verwendete Liste ist jederzeit in der Datenschutzerklärung auf fahrpilot.pro einsehbar und kann in Textform beim Auftragsverarbeiter angefragt werden.

— Ende des Vertrages —