Cursio

Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

24.06.2026

Zwischen

Verantwortlicher

Die Angaben des Verantwortlichen (Firmenname, Anschrift, gesetzliche Vertretung, USt-ID/HRB) ergeben sich aus dem Cursio-Kundenkonto des Verantwortlichen zum Zeitpunkt der elektronischen Annahme dieses Vertrages. Sie werden dort verpflichtend hinterlegt und in der Annahme-Bestätigung dokumentiert. Ein manuelles Ausfüllen dieses Feldes ist nicht erforderlich.

— nachfolgend „Verantwortlicher" genannt —

und

Auftragsverarbeiter

Blackfield Holding UG (haftungsbeschränkt) Industriestraße 13 65439 Flörsheim Handelsregister: Amtsgericht Wiesbaden, HRB 34886 Vertreten durch: Jonas Kunkel

— nachfolgend „Auftragsverarbeiter" oder „Cursio" genannt —

— gemeinsam „die Parteien" genannt —

Präambel

Der Verantwortliche nutzt die vom Auftragsverarbeiter betriebene Software-as-a-Service-Plattform „Cursio" (nachfolgend „Plattform") auf Grundlage der zwischen den Parteien geschlossenen Nutzungsvereinbarung (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-Buchungs- und Verwaltungsplattform für Kurse, Termine, Buchungen, Zahlungen und Kundenkommunikation).

(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 AVV 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 — Buchungsbelege, Rechnungen, Handelsbriefe: bis zu 10 Jahre) einer Löschung entgegensteht. Für die Dauer solcher Aufbewahrungspflichten bleiben die Daten in einem gesperrten, ausschließlich Aufbewahrungszwecken dienenden Zustand gespeichert. Vor der Löschung räumt der Auftragsverarbeiter dem Verantwortlichen eine Frist von 30 Kalendertagen zur eigenständigen Datensicherung ein; diese Frist beginnt mit dem Wirksamwerden der Vertragsbeendigung. Wünscht der Verantwortliche eine über die reine Bereitstellung im Kundenkonto hinausgehende Datenrückgabe (z. B. individuelle Export-Formate, Datenträger-Versand), trägt er den hierdurch entstehenden Aufwand des Auftragsverarbeiters. Backups im Rahmen des normalen Backup-Zyklus werden durch die reguläre Rotation überschrieben; eine sofortige, außerplanmäßige Backup-Löschung 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 Kundenkonto 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 oder Standard-Data-Processing-Addendum, 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, soweit vorhanden.

(3) Die vertraglichen Vereinbarungen des Auftragsverarbeiters mit seinen Unter-Auftragsverarbeitern — einschließlich ihres Wortlauts, ihrer Existenz im Einzelfall 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 berechtigte, 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, Video-Konferenzen und Live-Bildschirmfreigaben 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 schriftlichen Vereinbarung. Überprüfungen bei Unter-Auftragsverarbeitern sind ausgeschlossen; diese liegen in der Verantwortung des Auftragsverarbeiters. Ordentliche Auskunftsverlangen sind auf einmal pro Kalenderjahr 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 mit Verarbeitung außerhalb der EU/EWR sowie die jeweilige Rechtsgrundlage sind in **Anhang 3** aufgeführt. Mit Annahme dieses Vertrages stimmt der Verantwortliche den dort aufgeführten Drittlandtransfers 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, insgesamt jedoch höchstens auf die Summe der vom Verantwortlichen in den letzten zwölf Monaten vor dem schadensauslösenden Ereignis an den Auftragsverarbeiter tatsächlich gezahlten Nettoentgelte aus dem Hauptvertrag; (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 (Verantwortlicher bestimmt Zweck und Mittel, 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 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 Ergänzungen von TOMs oder Präzisierungen ohne Absenkung des Schutzniveaus) werden im Kundenkonto oder 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.

Verantwortlicher

Die Annahme dieses Vertrages erfolgt durch den Verantwortlichen elektronisch durch Klick auf „Ich akzeptiere den AVV" auf `cursio.pro/rechtliches/avv` (Login als Studio erforderlich). Diese Form genügt der Textform gemäß § 126b BGB und begründet einen wirksamen Vertragsschluss. Alternativ ist eine formlose Bestätigung per E-Mail an `hello@cursio.pro` mit dem Wortlaut „AVV in der Fassung vom 24.06.2026 akzeptiert" ausreichend.

Die elektronische Annahme wird vom Auftragsverarbeiter unter Angabe von Zeitstempel, akzeptierender Nutzer-Kennung, Studio-Zuordnung und akzeptierter Vertragsversion dokumentiert. Der Verantwortliche erhält eine Bestätigungs-Mail mit seinen aus dem Kundenkonto übernommenen Firmendaten und dem Annahmezeitpunkt als Nachweis für seinen Ordner.

Auftragsverarbeiter

Blackfield Holding UG (haftungsbeschränkt), vertreten durch Jonas Kunkel, Geschäftsführer Flörsheim, 24.06.2026

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

Anhang 1 — Art, Zweck, Datenkategorien und betroffene Personen

1. Zweck der Verarbeitung

Betrieb einer Online-Buchungs- und Verwaltungsplattform für Kurs- und Terminanbieter (insbesondere Yoga-, Pilates- und Fitness-Studios), einschließlich:

- Anlage und Verwaltung von Kursen, Terminen und Ressourcen
- Buchungsabwicklung und Zahlungsabwicklung (Weiterleitung an Zahlungsdienstleister)
- Kunden-, Mitgliedschafts- und Kartenverwaltung des Verantwortlichen
- Terminerinnerungen, Bestätigungen und sonstige transaktionale Kommunikation
- Bewertungs- und Feedbackverwaltung
- Bereitstellung von Rechnungen und buchhalterischen Auswertungen
- Fehleranalyse und Sicherstellung des Plattformbetriebs

2. Art der Verarbeitung

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

3. Kategorien personenbezogener Daten

Kategorie	Beispiele
Stammdaten Kundinnen und Kunden	Name, Anrede, E-Mail-Adresse, Telefonnummer, Rechnungs- und Lieferadresse, Geburtsdatum (optional)
Konto- und Zugangsdaten	Benutzer-ID, verschlüsselte Passwörter, Login-Zeitpunkte, Zwei-Faktor-Konfiguration
Buchungs- und Nutzungsdaten	Kurs- und Terminbuchungen, Check-ins, Stornierungen, Wartelisten, Karten- und Mitgliedschaftsstände
Zahlungsdaten	Zahlungsstatus, Beleg- und Rechnungsnummern, Referenzen zu Zahlungsdienstleister-Transaktionen (die eigentlichen Zahlungsmittel-Daten liegen beim Zahlungsdienstleister)
Kommunikationsdaten	Versendete transaktionale E-Mails, Push-Benachrichtigungen, In-App-Nachrichten
Freiwillige Angaben	Bewertungen, Notizen des Verantwortlichen zu seinen Kundinnen und Kunden, Profilbilder
Technische Daten	IP-Adressen, Geräte- und Browserdaten, Zeitstempel — soweit zur Sicherstellung des Betriebs erforderlich
Mitarbeiterdaten des Verantwortlichen	Name, E-Mail-Adresse, Rolle und Berechtigungen von Trainerinnen, Trainern und Verwaltungspersonal

4. Kategorien betroffener Personen

- Kundinnen und Kunden (Teilnehmerinnen und Teilnehmer) des Verantwortlichen
- Mitarbeiterinnen und Mitarbeiter des Verantwortlichen (Trainer, Verwaltung, Empfang)
- Interessentinnen und Interessenten, die über die Plattform Kontakt aufnehmen

---

Anhang 2 — Technische und organisatorische Maßnahmen (TOM)

Gemäß Art. 32 DSGVO trifft der Auftragsverarbeiter folgende technische und organisatorische 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 Hosting-Unter-Auftragsverarbeitern in EU-Rechenzentren betrieben (siehe Anhang 3). Diese verfügen über eigene Zutrittskontrollen (u. a. Vereinzelungsanlagen, Videoüberwachung, 24/7-Sicherheitspersonal).

1.2 Zugangskontrolle

- Zugriff auf Produktivsysteme nur über verschlüsselte Verbindungen (mindestens TLS 1.3, TLS 1.2 nur als Fallback)
- Persönliche, individuelle Zugangsdaten für alle Personen mit Systemzugriff
- Zwei-Faktor-Authentifizierung (2FA) verpflichtend für alle administrativen Zugänge
- Passwort-Anforderungen nach aktueller BSI-Empfehlung (Mindestlänge, Komplexität, keine Wiederverwendung)
- Automatische Sitzungsbeendigung nach Inaktivität
- Verschlüsselung ruhender Daten (encryption-at-rest) durch die eingesetzten Hosting-Unter-Auftragsverarbeiter (AES-256 oder gleichwertig)

1.3 Zugriffskontrolle

- Rollen- und rechtebasierte Zugriffsberechtigungen auf Ebene der Datenbank (Row-Level-Security)
- Trennung von Produktiv-, Test- und Entwicklungsumgebungen
- Vier-Augen-Prinzip bei Änderungen an der Produktivdatenbank durch Deployment-Freigaben
- Protokollierung aller administrativen Zugriffe

1.4 Trennungskontrolle

- Mandantenfähige Datenhaltung: Daten verschiedener Verantwortlicher werden logisch getrennt gespeichert und abgefragt
- Trennung von Produktions-, Test- und Entwicklungsdaten
- Getrennte Datenbank-Rollen für unterschiedliche Zugriffszwecke

1.5 Pseudonymisierung

- Interne Kennungen (UUIDs) statt sprechender IDs
- Fehler-Logs werden vor Übermittlung an das Monitoring-System um personenbezogene Daten bereinigt (PII-Redaktion)

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

2.1 Weitergabekontrolle

- Verschlüsselte Übertragung sämtlicher Daten zwischen Endgerät und Plattform (HTTPS/TLS 1.2 oder höher)
- Verschlüsselte Übertragung zwischen internen Systemen (Datenbank, Anwendung, Zahlungsdienstleister)
- Datenübermittlung an Unter-Auftragsverarbeiter nur über gesicherte, vertraglich abgesicherte Schnittstellen

2.2 Eingabekontrolle

- Protokollierung sicherheitsrelevanter Änderungen an Datensätzen (Audit-Logs)
- Änderungen an kritischen Datensätzen (Buchungen, Zahlungen, Löschungen) mit Zeitstempel und Nutzerkennung nachvollziehbar
- Versionierung von Software-Änderungen über Git

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

- Betrieb auf redundanter Cloud-Infrastruktur in EU-Rechenzentren
- Automatische Datenbank-Backups mindestens täglich mit einer Aufbewahrungsdauer von mindestens 7 Tagen (Standard: 30 Tage, Point-in-Time-Recovery über den vom Hosting-Unter-Auftragsverarbeiter angebotenen Zeitraum)
- Monitoring der Systemverfügbarkeit und Alarmierung bei Ausfällen
- Verschlüsselte Speicherung von Backups
- Wiederherstellungsverfahren werden dokumentiert und regelmäßig überprüft

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

- Regelmäßige Überprüfung der eingesetzten Unter-Auftragsverarbeiter und deren Datenschutz-Nachweise (Zertifikate, DPA-Dokumentation)
- Fortlaufende Aktualisierung von Systemen und Bibliotheken (Sicherheits-Updates)
- Automatisierte Sicherheits-Scans des Quellcodes und der Abhängigkeiten
- Dokumentation aller Verarbeitungstätigkeiten
- Sicherheitsvorfälle werden dokumentiert und ausgewertet

5. Auftragskontrolle (Art. 28 DSGVO)

- Bindung aller Unter-Auftragsverarbeiter durch individuelle Auftragsverarbeitungsverträge oder durch Zugrundelegung ihrer Standard-Datenschutzbedingungen, die den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechen
- Prüfung und Dokumentation der TOM der Unter-Auftragsverarbeiter vor Beauftragung anhand öffentlich verfügbarer Zertifikate, Testate oder eigener Datenschutz-Dokumentation
- Weisungen an Mitarbeitende zur ausschließlich weisungsgebundenen Verarbeitung

6. Datenschutzbeauftragter

Der Auftragsverarbeiter ist nicht gemäß Art. 37 DSGVO bzw. § 38 BDSG zur Bestellung eines Datenschutzbeauftragten verpflichtet, da weder die Kerntätigkeit in einer umfangreichen regelmäßigen und systematischen Überwachung betroffener Personen besteht noch die Kerntätigkeit in einer

umfangreichen Verarbeitung besonderer Datenkategorien liegt, noch die Mitarbeiterzahl den Schwellenwert des § 38 BDSG erreicht. Datenschutzanfragen sind an die im Impressum der Plattform hinterlegte Kontaktadresse zu richten.

Anhang 3 — Liste der Unter-Auftragsverarbeiter

Der Auftragsverarbeiter setzt zum Zeitpunkt des Vertragsschlusses folgende Unter-Auftragsverarbeiter ein. Die Bindung dieser Unter-Auftragsverarbeiter erfolgt gemäß § 5 Abs. 4 dieses Vertrages entweder durch individuellen Auftragsverarbeitungsvertrag oder durch Zugrundelegung der jeweiligen Standard-Datenschutzbedingungen des Unter-Auftragsverarbeiters, die den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechen.

#	Unter-Auftragsverarbeiter	Sitz	Ort der Verarbeitung	Leistung	Bindung / Rechtsgrundlage
1	**Vercel Inc.**	Walnut, CA, USA	EU (Frankfurt-Region)	Hosting der Web-Anwendung, Content Delivery	Standard-DPA des Anbieters (akzeptiert), EU-Region konfiguriert; ergänzend Standardvertragsklauseln für etwaige Drittlandverarbeitung
2	**Supabase Inc.**	Wilmington, DE, USA (EU-Entity Supabase EU)	EU (Frankfurt-Region über AWS)	Datenbank (PostgreSQL), Authentifizierung, Datei-Speicher	Standard-DPA des Anbieters (akzeptiert), EU-Verarbeitung
3	**Resend, Inc.**	San Francisco, CA, USA	USA (EU-Region in Vorbereitung)	Transaktionale E-Mail-Zustellung	Standard-DPA des Anbieters (akzeptiert), EU-US Data Privacy Framework, Standardvertragsklauseln
4	**Stripe Payments Europe, Ltd.**	Dublin, Irland (Gruppen-Affiliates u. a. USA)	EU (Irland), teilweise USA bei internationalen Kartennetzwerken	Zahlungsabwicklung, Auszahlungen an den Verantwortlichen, Rechnungsstellung	Standard-Services-Agreement (SSA) mit integriertem DPA, EU-Verarbeitung; für erforderliche Drittlandtransfers Standardvertragsklauseln des Anbieters
5	**Functional Software, Inc. (Sentry)**	San Francisco, CA, USA	USA (bzw. konfigurierte EU-Region)	Fehler-Monitoring; PII-Redaktion aktiv	Standard-DPA des Anbieters (akzeptiert), EU-US Data Privacy Framework, Standardvertragsklauseln

6	**Upstash, Inc.**	Walnut, CA, USA	EU (Frankfurt-Region)	Redis-Cache, Rate-Limiting	Standard-DPA des Anbieters (bereitgestellt), EU-Verarbeitung; ergänzend Standardvertragsklauseln
7	**Cloudflare, Inc.**	San Francisco, CA, USA	Global (u. a. EU)	Bot-Schutz (Turnstile), CDN	Standard-DPA des Anbieters (im Cloudflare-Dashboard verfügbar), EU-US Data Privacy Framework, Standardvertragsklauseln
8	**Google Ireland Limited**	Dublin, Irland (Konzern-Affiliates u. a. USA)	EU (Irland), teilweise USA	Karten-Darstellung (Google Maps), OAuth-Login (Google Sign-In), Web-Fonts	Standard-DPA des Anbieters (per Google-Cloud-Projekt akzeptiert), EU-Verarbeitung / für Drittlandtransfers Standardvertragsklauseln

Änderungen dieser Liste werden dem Verantwortlichen gemäß § 5 Abs. 2 dieses Vertrages mitgeteilt. Der Verantwortliche kann die aktuell verwendete Liste jederzeit im Kundenkonto oder auf Anfrage in Textform beim Auftragsverarbeiter abrufen.

Ende des Vertrages