Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 EU-DSGVO

Vereinbarung

zwischen dem/der Verantwortlichen

- nachstehend *Auftraggeber* genannt -

und dem/der Auftragsverarbeiter/in

Fyndery GmbH, Agnes-Pütreich-Straße 70, 93053 Regensburg

- nachstehend *Auftragnehmer* genannt -

Hinweis

Diese Vereinbarung ist als Ergänzung zum bestehenden Hauptvertrag zwischen Auftragnehmer und Auftraggeber zu verstehen.

1. Gegenstand des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Es wird die Buchungssoftware „Fyndery Buchungstool“ zur Verfügung gestellt. Diese wird für die Kurs- und Teilnehmerverwaltung sowie für die Erstellung, Bewerbung und Abrechnung der Kurse/Angebote auf der Website des Auftraggebers sowie auf der eigenen Plattform des Auftragnehmers, dem so genannten „Marktplatz“ genutzt. Der Auftrag beinhaltet somit die Speicherung, Aktualisierung, Übertragung und Löschung von Teilnehmerdaten, eventuell den Export von Teilnehmerdaten, die Kursverwaltung und Übertragung von Kursdaten, die Bearbeitung von Support-Anfragen.

Der Auftragnehmer bietet darüber hinaus die Übernahme der Kundenkommunikation, wie z.B. den Newsletterversand an.

Zudem bietet der Auftragnehmer das Erstellen und Pflegen der Partner-Websites an.

(2) Zweck

Der Auftrag dient zur Erfüllung der folgenden Zwecke:

Buchungsabwicklung, Transaktions-/Zahlungsabwicklung, Teilnehmerverwaltung, Partnerverwaltung, Auswertungen, Teilnehmerkommunikation (Newsletter-Anmeldungen).

(3) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(4) Ort der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich in Deutschland sowie in Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum.

Soweit Unterauftragnehmer im Vereinigten Königreich eingesetzt werden, erfolgt die Datenverarbeitung auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission gemäß Art. 45 DSGVO.

Soweit eine Verarbeitung personenbezogener Daten in den Vereinigten Staaten von Amerika oder in einem sonstigen Drittland erfolgt, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden. Die Übermittlung erfolgt in diesen Fällen auf Grundlage geeigneter Garantien, insbesondere durch Abschluss von Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO oder auf Grundlage eines gültigen Angemessenheitsbeschlusses.

Eine darüberhinausgehende Übermittlung in Drittländer erfolgt nicht.

(5) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Bilddaten (Profilbild), Geschlecht, Geburtsdatum

(6) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☒ Interessenten
- ☒ Ansprechpartner
- ☒ Partner

2. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c sowie Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Anlage TOM).
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Der Auftraggeber ist selbstständig für die zeitgerechte Löschung von Daten verantwortlich.
(3) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartnerin beim Auftragnehmer wird Frau Madlen Bauer, datenschutz@fyndery.de benannt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in Anlage TOM).
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

5. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen,

Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Bei Vertragsschluss bestehen bereits folgende Unterauftragsverhältnisse, deren Beauftragung der Auftraggeber mit Unterzeichnung dieser Vereinbarung unter der Bedingung des Vorhandenseins einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO bzw. des Art. 44 ff. DSGVO, zustimmt:

Firma Unterauftrag-nehmer	Anschrift/Land	Leistung	Betroffene Daten
PythonAnywhere LLP	5 The Green Richmond TW9 1PL United Kingdom	Hosting der Website des Auftragnehmers	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Bilddaten, Geschlecht, Geburtsdatum
BunnyWay d.o.o. (Bunny CDN)	Dunajska cesta 165 1000 Ljubljana Slowenien	Hosting im Rahmen des Baukasten-systems für Partner-Websites	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten sowie sonstige Daten, die im Rahmen der Nutzung der Partner-Websites verarbeitet werden
Stripe Payments Europe Ltd.	1 Grand Canal Street Lower Grand Canal Dock Dublin 2 Irland	Zahlungsabwicklung, Transaktionsverarbeitung und technische Abwicklung von Online-Zahlungen	Personenstammdaten, Kommunikationsdaten, Vertragsabrechnungs- und Zahlungsdaten, Transaktionsdaten
Acumbamail S.L.	C/ Santa Teresa, 1 02002 Albacete Spanien	Newsletter-Versand und Newsletter-Analyse	E-Mail-Adressen, Personenstammdaten, Kommunikationsdaten, Nutzungsdaten im Zusammenhang mit Newsletter-Kampagnen
Calendly LLC	271 17th St NW 10th Floor Atlanta, GA 30363 USA	Terminbuchung und Terminverwaltung	Personenstammdaten, Kommunikationsdaten, Termin- und Kalendereinträge

Soweit Zahlungsdienstleister personenbezogene Daten zur Erfüllung eigener gesetzlicher

Verpflichtungen verarbeiten, insbesondere zur Betrugsprävention, Geldwäschebekämpfung oder aufsichtsrechtlichen Anforderungen, handeln diese insoweit als eigenständige Verantwortliche.
(3) Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt *und*

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftragnehmers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Abweichend hiervon bleibt die Verantwortung für die Zulässigkeit einer solchen Leistung beim Auftraggeber, soweit es sich um eine vom Auftraggeber explizit gewünschte Leistung handelt.
(6) Eine weitere Auslagerung durch den Unterauftragnehmer ist nur unter den unter Abs. 3 genannten Bedingungen gestattet. Sämtliche vertragliche Regelungen in der Vertragskette sind auch den weiteren Unterauftragnehmern aufzuerlegen.

6. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Stichprobenkontrollen sind zulässig, sofern ein berechtigter Anlass besteht. Sie sind mit angemessener Vorankündigung durchzuführen und dürfen den Geschäftsbetrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis allgemeiner Maßnahmen sowie solcher, welche den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Im Falle einer Unterstützungsleistung werden die Parteien eine angemessene Vergütung der Tätigkeiten des Auftragnehmers vereinbaren.

8. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers im Sinne des Art. 28 DSGVO. Weisungen können in Textform, insbesondere per E-Mail, erfolgen.

(2) Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(3) Weisungsberechtigt sind die vertretungsberechtigten Personen des Auftraggebers sowie von diesem ausdrücklich benannte Personen. Weisungen sind an die vom Auftragnehmer benannte Kontaktadresse zu richten.

(4) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Der

Auftragnehmer ist in diesem Fall berechtigt, die Durchführung der Weisung bis zur Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Dem Auftragnehmer wird gestattet, die im Auftrag verarbeiteten personenbezogenen Daten nach Beendigung dieser Vereinbarung im Sinne der DSGVO vollständig zu anonymisieren, die anonymisierten Daten weiter zu speichern und auszuwerten. Eine Identifizierbarkeit von Personen muss hierbei praktisch unmöglich sein. Die Anonymisierung erfolgt irreversibel und nach dem Stand der Technik. Die Art und Weise der Anonymisierung wird dem Auftraggeber mitgeteilt. Nach Abschluss der Anonymisierung sind die im Auftrag verarbeiteten personenbezogenen Daten nach dieser Vorschrift zu löschen oder zurückzugeben.
(3) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Stand: Juli 2026