Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO

Status	Entwurf zur rechtlichen Prüfung
Version	0.0.1
Auftragnehmer	Qourses UG (haftungsbeschränkt)
Vertreten durch	Geschäftsführer Dennis von der Bey

Auftraggeber

Name / Kundename

Rechtlicher Name / Firma

Anschrift

Vertretungsberechtigte Person

Auftragnehmer
Qourses
Qourses UG (haftungsbeschränkt)
Hauptstraße 123, 45219 Essen
Vertreten durch: Dennis von der Bey, Geschäftsführer

Gegenstand und Dauer

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch Qourses UG (haftungsbeschränkt) als Auftragnehmer für den Auftraggeber im Zusammenhang mit der Nutzung der Qourses-Plattform für Kursbuchung, Teilnehmerverwaltung, Zahlungs- und Kommunikationsprozesse sowie damit zusammenhängenden kundenindividuellen Erweiterungen, Integrationen und Support- oder Entwicklungsleistungen.
Der Vertrag beginnt am 2026-07-01 und gilt für die Dauer des Hauptvertrags über die Nutzung von Qourses. Kündigungs- und Löschpflichten aus diesem Vertrag bleiben unberührt.

Art und Zweck der Verarbeitung

Die Verarbeitung dient der Bereitstellung eines Software-as-a-Service-Angebots für Kursanbieter einschließlich plattformbezogener Individualsoftware, Anpassungen und Integrationen. Qourses verarbeitet personenbezogene Daten nur dokumentiert und weisungsgebunden, soweit dies für Betrieb, Wartung, Support, Entwicklung, Fehleranalyse, Sicherheit und Vertragserfüllung erforderlich ist.

Weisungen des Auftraggebers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern keine gesetzliche Pflicht zur Verarbeitung besteht. Weisungen können im Hauptvertrag, in diesem Vertrag, über Administrationsfunktionen der Plattform oder in Textform erteilt werden.
Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, informiert er den Auftraggeber hierüber unverzüglich. Der Auftragnehmer ist berechtigt, die Ausführung der betroffenen Weisung auszusetzen, bis der Auftraggeber sie bestätigt, ändert oder zurücknimmt.

Vertraulichkeit

Der Auftragnehmer verpflichtet alle zur Verarbeitung befugten Personen auf Vertraulichkeit, soweit keine gesetzliche Verschwiegenheitspflicht besteht. Der Zugriff wird auf Personen beschränkt, die ihn für Betrieb, Support oder Wartung benötigen.
Der Auftragnehmer trifft angemessene Maßnahmen, damit nur solche Mitarbeitende, Dienstleister und Organe Zugriff auf personenbezogene Daten erhalten, die diesen Zugriff zur Erfül-

lung ihrer Aufgaben benötigen. Zugriffsbefugnisse werden nach Aufgabenbezug vergeben und bei Wegfall der Erforderlichkeit entzogen.
Die Vertraulichkeitsverpflichtungen bestehen auch nach Ende des Vertrags fort, soweit die betroffenen Personen nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die bei Vertragsschluss maßgeblichen Maßnahmen sind in Anlage 2 beschrieben. Der Auftragnehmer darf Maßnahmen weiterentwickeln, sofern das Schutzniveau nicht wesentlich unterschritten wird.
Der Auftragnehmer überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig und passt sie an, soweit dies unter Berücksichtigung von Risiko, Stand der Technik, Art der Verarbeitung und verfügbaren Informationen erforderlich ist.

Pflichten des Auftraggebers und Kontaktstellen

Der Auftraggeber bleibt für die Rechtmäßigkeit der Verarbeitung, die Zulässigkeit der Weisungen, die Erfüllung der Informationspflichten gegenüber betroffenen Personen und die Beantwortung von Betroffenenanfragen verantwortlich, soweit dieser Vertrag nichts anderes regelt.
Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler, Unregelmäßigkeiten oder datenschutzrechtliche Risiken in Auftragsergebnissen oder im Zusammenhang mit der Leistungserbringung feststellt.
Kontaktstelle des Auftraggebers für datenschutzbezogene Vertragsfragen ist die im Parteienblock benannte Vertretung, sofern der Auftraggeber keine andere Kontaktstelle in Textform mitteilt. Kontaktstelle des Auftragnehmers ist Dennis von der Bey, Geschäftsführer, sofern der Auftragnehmer keine andere Kontaktstelle in Textform mitteilt. Eine Benennung als Datenschutzbeauftragter ist damit nicht verbunden.

Unterauftragsverarbeiter

Der Auftraggeber genehmigt die in Anlage 3 aufgeführten Unterauftragsverarbeiter. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen, sodass der Auftraggeber aus wichtigem datenschutzrechtlichem Grund widersprechen kann.
Der Auftragnehmer schließt mit Unterauftragsverarbeitern Vereinbarungen, die ein im Wesentlichen gleichwertiges Datenschutzniveau sicherstellen. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die datenschutzkonforme Leistungserbringung der eingesetzten Unterauftragsverarbeiter verantwortlich.
Beabsichtigte neue oder ersetzende Unterauftragsverarbeiter werden dem Auftraggeber mindestens 30 Tage vor Einsatz in geeigneter Form mitgeteilt. Widerspricht der Auftraggeber aus wichtigem datenschutzrechtlichem Grund, bemühen sich die Parteien um eine angemessene Lösung; ist eine solche nicht möglich, kann der Auftraggeber die betroffenen Leistungen beenden, soweit sie den neuen Unterauftragsverarbeiter zwingend erfordern.

Betroffenenrechte und Mitwirkung

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung angemessen bei der Erfüllung von Betroffenenrechten, Datenschutz-Folgenabschätzungen, Meldungen von Datenschutzverletzungen und Nachweispflichten.
Gehen Anfragen betroffener Personen unmittelbar beim Auftragnehmer ein und kann der Auftragnehmer diese dem Auftraggeber zuordnen, leitet der Auftragnehmer die Anfrage an den Auftraggeber weiter oder verweist die betroffene Person auf den Auftraggeber, soweit der Auftragnehmer nicht zur eigenen Bearbeitung berechtigt oder verpflichtet ist.

Datenschutzverletzungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die Daten des Auftraggebers

betrifft. Die Mitteilung enthält, soweit verfügbar, Art der Verletzung, betroffene Daten- und Personenkategorien, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen sowie eine Kontaktstelle für Rückfragen.
Der Auftragnehmer unterstützt den Auftraggeber angemessen bei Untersuchung, Eindämmung, Abhilfe und Erfüllung gesetzlicher Melde- und Benachrichtigungspflichten. Informationen können schrittweise ergänzt werden, wenn sie zum Zeitpunkt der ersten Meldung noch nicht vollständig vorliegen.

Datenschutz-Folgenabschätzung und Behörden

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der verfügbaren Informationen angemessen bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen mit Aufsichtsbehörden, soweit sich die Unterstützung auf die Verarbeitung durch den Auftragnehmer bezieht.

Löschung und Rückgabe

Nach Ende der Leistungserbringung löscht oder gibt der Auftragnehmer personenbezogene Daten nach Wahl des Auftraggebers zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Details sind in Anlage 4 geregelt.

Nachweise und Audits

Der Auftragnehmer stellt dem Auftraggeber die erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrags bereit. Audits erfolgen nach vorheriger Abstimmung, während üblicher Geschäftszeiten und unter Wahrung von Sicherheit, Vertraulichkeit und Betriebsstabilität.
Audits sind vorrangig durch Dokumentenprüfung, Sicherheitsnachweise, Auskünfte oder Remote-Termine durchzuführen. Da der Auftragnehmer seine Leistungen remote und mit Cloud-Anbietern erbringt, sind physische Vor-Ort-Prüfungen beim Auftragnehmer nur erforderlich, soweit ein gleichwertiger Nachweis nicht remote erbracht werden kann und die Prüfung rechtlich geboten ist. Der Auftragnehmer darf Nachweise schwärzen, soweit dies zum Schutz von Betriebsgeheimnissen, Sicherheitsinformationen, Daten anderer Kunden oder gesetzlichen Pflichten erforderlich ist.
Prüfungen durch Datenschutzaufsichtsbehörden oder andere zuständige hoheitliche Stellen bleiben unberührt. Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang, soweit sich die Prüfung auf die Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer bezieht.

Internationale Datenübermittlungen

Eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Soweit erforderlich, stützt der Auftragnehmer solche Übermittlungen auf einen Angemessenheitsbeschluss, Standardvertragsklauseln der Europäischen Kommission oder einen anderen zulässigen Transfermechanismus.
Setzt ein Unterauftragsverarbeiter Standardvertragsklauseln oder zusätzliche Schutzmaßnahmen ein, stellt der Auftragnehmer die hierfür erforderlichen Informationen in angemessenem Umfang bereit. Details zu bekannten Transferbezügen ergeben sich aus Anlage 3 und Anlage 5.

Gefährdung durch Dritte

Werden personenbezogene Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, Insolvenzverfahren, behördliche Maßnahmen oder sonstige Ereignisse Dritter gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich, soweit dies rechtlich zulässig ist. Der Auftragnehmer weist die beteiligten Stellen, soweit möglich und rechtlich zulässig, darauf hin, dass die Verantwortung für die Daten beim Auftraggeber liegt.

Haftung

Für die Haftung der Parteien gelten die gesetzlichen Vorschriften, insbesondere Art. 82 DSGVO, sowie die Haftungsregelungen des Hauptvertrags, soweit dieser Vertrag nichts Abweichendes regelt. Die datenschutzrechtlichen Pflichten aus diesem Vertrag bleiben hiervon unberührt.

Schlussbestimmungen

Änderungen dieses Vertrags bedürfen der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist. Bei Widersprüchen gehen die Regelungen dieses Vertrags den datenschutzbezogenen Regelungen des Hauptvertrags vor. Soweit Standardvertragsklauseln anwendbar sind, gehen diese bei Widersprüchen den übrigen Regelungen dieses Vertrags vor.

Ort, Datum, Unterschrift Auftraggeber

Ort, Datum, Unterschrift Auftragnehmer
Dennis Michael von der Bey, Geschäftsführer

Anlage 1: Beschreibung der Verarbeitung

Verarbeitungszwecke

Bereitstellung der Qourses-Plattform für Kursbuchung, Teilnehmerverwaltung, Kommunikation, Abrechnung, Support, Fehleranalyse und Sicherheit einschließlich damit zusammenhängender kundenindividueller Erweiterungen, Integrationen und Entwicklungsleistungen.

Kategorien betroffener Personen

Administratoren und Mitarbeitende des Auftraggebers, Kursteilnehmer, Interessenten und Kommunikationspartner.

Datenkategorien

Stammdaten, Kontaktdaten, Kurs- und Buchungsdaten, Kommunikationsdaten, Zahlungsstatus, technische Nutzungs- und Protokolldaten.

Verarbeitungstätigkeiten

Erheben, Speichern, Strukturieren, Anzeigen, Übermitteln, Abgleichen, Einschränken, Löschen, Exportieren, Importieren, Migrieren, Testen und Fehleranalysieren im Rahmen der Plattformfunktionen und damit zusammenhängender Individualleistungen.

Dauer der Verarbeitung

Für die Dauer des Hauptvertrags sowie anschließend nur, soweit Rückgabe, Export, Löschung, gesetzliche Aufbewahrung oder Nachweiszwecke dies erfordern.

Rechte und Pflichten des Auftraggebers

Der Auftraggeber bleibt für Rechtmäßigkeit, Weisungen, Betroffeneninformationen, Kontaktstellen, Mitteilung erkannter Unregelmäßigkeiten und die Wahrnehmung der Verantwortlichenpflichten verantwortlich.

Anlage 2: Technische und organisatorische Maßnahmen

Zugriffskontrolle

Rollen- und berechtigungsbasierter Zugriff, administrative Konten nur für berechtigte Personen, Entzug nicht mehr benötigter Berechtigungen und starke Authentisierung für interne Systeme soweit verfügbar.

System- und Datenzugriff

Mandantenbezogene Zugriffsbeschränkungen in der Anwendung, beschränkter administrativer Zugriff auf Produktivsysteme, Protokollierung relevanter Betriebs- und Sicherheitsereignisse und Zugriff nur nach Aufgabenbezug.

Transport- und Speicherschutz

Verschlüsselte Übertragung per TLS, kontrollierte Produktivkonfigurationen, getrennte Mandantenlogik, gesicherte Secrets und begrenzter Zugriff auf Datenbanken, Queues und Speicherorte.

Eingabe- und Änderungskontrolle

Nachvollziehbare technische Betriebsprotokolle, versionierte Infrastruktur- und Anwendungskonfigurationen sowie dokumentierte Änderungsprozesse für produktionsrelevante Systeme.

Verfügbarkeit

Betriebsüberwachung, Fehlerprotokollierung, Backup- und Wiederherstellungsprozesse, Schutz vor unbeabsichtigter Zerstörung oder Verlust und Nutzung verwalteter Infrastruktur mit angemessenen Verfügbarkeitsmaßnahmen.

Trennung und Minimierung

Mandantenlogik zur Trennung von Kundenkontexten, zweckbezogene Verarbeitung, beschränkte Support- und Entwicklungszugriffe, Vermeidung unnötiger Produktivdatenkopien und bevorzugte Nutzung anonymisierter oder synthetischer Daten für Entwicklung und Tests, soweit dies möglich ist.

Incident- und Schwachstellenmanagement

Dokumentierte Support- und Incident-Prozesse, Sicherheitsupdates im Rahmen des Betriebs, Auswertung relevanter Fehler- und Sicherheitsmeldungen und Eskalation bei Datenschutzverletzungen.

Organisation

Vertraulichkeitsverpflichtungen, datenschutzbewusste Entwicklung, beschränkter Zugang zu internen Systemen und regelmäßige Überprüfung der Wirksamkeit der Maßnahmen.

Anlage 3: Unterauftragsverarbeiter

Anbieter	Leistung / Datenkategorien	Ort der Verarbeitung / Hinweise
Fly.io	Hosting der Qourses API und Backend-Ausführung; Verkehrs-, Authentifizierungs-, Kurs-, Buchungs-, Zahlungsstatus- und Supportdaten, soweit über die API verarbeitet.	Hosting innerhalb der jeweils eingesetzten Anbieterregionen; Einsatz nach Anbieterbedingungen und vereinbartem Transfermechanismus.
Crunchy Bridge	Managed PostgreSQL für Anwendungsdaten; Organisationen, Nutzer, Kurse, Termine, Buchungen, Bestellungen, Zahlungsreferenzen, Benachrichtigungs- und Audit-/Betriebsdaten.	Betrieb in einer EU-Region, derzeit Deutschland, über den Managed-Database-Anbieter.
MongoDB Atlas	Managed MongoDB für Hintergrundjobs / Pulse; Job-Metadaten, Zeitpläne und technische Verarbeitungsdaten.	Betrieb in einer EU-Region, derzeit Deutschland, über den Managed-Database-Anbieter.
CloudAMQP	Managed RabbitMQ für asynchrone Verarbeitung und Benachrichtigungsqueues; technische Nachrichten zu E-Mail-, Push-, Buchungs- und Plattformereignissen.	Betrieb in einer EU-Region, derzeit Deutschland, über den Managed-Queue-Anbieter.
Cloudflare	DNS, Reverse Proxy/CDN, Pages Hosting, Images, Turnstile und RealtimeKit; IP-/Requestdaten, Webseitenaufrufe, hochgeladene Bilder, Captcha-Token, Meeting-/Teilnehmer-Token und ggf. Audio-/Videodaten bei Online-Kursräumen.	Einsatz für `qours.es`, `app.qours.es`, API-Proxied Traffic, Shortlinks, Bilder und optionale Online-Kursräume nach Cloudflare-Vertragsunterlagen.
Auth0	Authentifizierung und Identitätsverwaltung; E-Mail-Adresse, Vorname, Nachname, Login-IDs, Rollen, Berechtigungen, Session- und Token-Metadaten.	Custom Domain `auth.qours.es`; Auth0 versendet Auth-E-Mails über Postmark.
Stripe	Zahlungsabwicklung, Stripe Connect, Checkout, Billing Portal und Webhooks; Organisations- und Zahlungsprofilinformationen, Rechnungs-/Zahlungsdaten, Zahlungsstatus, Stripe-IDs und ggf. Teilnehmer-/Bestellbezug.	Einsatz für Qourses-Abos und Kurszahlungen; Stripe kann je nach Zahlungsfluss eigenständig Verantwortlicher sein.
Postmark	Transaktionaler E-Mail-Versand; E-Mail-Adressen, Namen, Buchungs-/Bestell-/Kursinformationen und Auth0-System-E-Mails.	Einsatz für transaktionale Plattform- und Authentifizierungs-E-Mails nach Anbieterbedingungen.

Anbieter	Leistung / Datenkategorien	Ort der Verarbeitung / Hinweise
Sentry	Fehleranalyse und Performance-Monitoring für Backend, Frontend, Mobile und Shortlinks; technische Fehlerdaten, User-Kontext, IP-/Requestdaten und maskierte Session-Replay-Daten.	Einsatz für Fehleranalyse und Monitoring; Inhalte werden nach Möglichkeit minimiert oder maskiert.
Better Stack / Better Uptime	Logging, Monitoring und Status Page; Backend-, Cloudflare-, Auth0- und Datenbanklogs sowie Uptime-Prüfungen.	Einsatz für Betriebsüberwachung, Log-Auswertung und Verfügbarkeitsprüfungen; Inhalte und Aufbewahrung richten sich nach Anbieterbedingungen und interner Konfiguration.
Google / Firebase Cloud Messaging	Android Push-Benachrichtigungen; Push-Token, technische Geräte-/Installationsdaten und Benachrichtigungsinhalte.	Einsatz abhängig von aktivierter Mobile-Push-Funktion und Anbieterbedingungen.
Apple Push Notification service	iOS Push-Benachrichtigungen; Push-Token, technische Geräte-/Installationsdaten und Benachrichtigungsinhalte.	Einsatz abhängig von Mobile-Push-Funktion.
Google Maps Platform	Ortsauswahl und Ortsreferenzen; eingegebene Such-/Ortsdaten, Place IDs und technische Nutzungsdaten.	Einsatz bei Standortsuche und Standortverwaltung nach Anbieterbedingungen.
Mapbox	Kartendarstellung; Standortkoordinaten, Kartenaufrufe und technische Nutzungsdaten.	Einsatz bei Kartendarstellung und standortbezogenen Plattformfunktionen nach Anbieterbedingungen.
Crisp	Support-Chat und Identitätsverifikation; Chat-Inhalte, E-Mail-Adresse bzw. Identifikationshash und technische Supportdaten.	Einsatz auf Qourses-Marketing-/Support-Oberflächen, soweit Support-Chat oder Support-Identifikation aktiviert ist.

Anlage 4: Löschung, Rückgabe, Audit und Support

Export

Der Auftraggeber kann verfügbare Plattformexporte nutzen oder einen angemessenen Export in Textform anfordern. Der konkrete Umfang richtet sich nach den Plattformfunktionen und den technisch verfügbaren Daten.

Rückgabe

Soweit der Auftraggeber Rückgabe verlangt, stellt der Auftragnehmer personenbezogene Daten in einem angemessenen, technisch verfügbaren Format bereit.

Löschung

Nach Vertragsende werden produktive personenbezogene Daten grundsätzlich innerhalb von 30 Tagen gelöscht oder zur Löschung vorgemerkt, soweit keine gesetzlichen Aufbewahrungspflichten, Sicherheitsanforderungen oder berechtigte Nachweiszwecke entgegenstehen.

Backups

Backups werden im regulären Sicherungszyklus überschrieben oder gelöscht und nur für Wiederherstellungs-, Sicherheits- und Betriebsstabilitätszwecke verwendet.

Bestätigung

Auf Anfrage bestätigt der Auftragnehmer die Durchführung der Löschung oder die fortbestehenden Gründe einer eingeschränkten Aufbewahrung in Textform.

Auditunterstützung

Anfragen werden über den Supportkanal koordiniert. Der Auftraggeber beschreibt Prüfungsgegenstand, Zeitraum und Anlass. Nachweise werden vorrangig durch Dokumente, Sicherheitsinformationen, Anbieterunterlagen, Auskünfte oder Remote-Termine bereitgestellt.

Kosten und Grenzen

Aufwände für außergewöhnliche Prüfungen oder individuelle Nachweise können nach vorheriger Abstimmung angemessen berechnet werden. Prüfungen dürfen Sicherheit, Verfügbarkeit, Betriebsgeheimnisse und Daten anderer Kunden nicht gefährden.

Support

Datenschutzbezogene Anfragen werden über den vereinbarten Support- oder Kontaktkanal koordiniert und nach Dringlichkeit sowie gesetzlicher Fristrelevanz priorisiert.

Anlage 5: Internationale Übermittlungen

Grundsatz

Drittlandübermittlungen erfolgen nur auf Grundlage der Art. 44 ff. DSGVO, insbesondere Angemessenheitsbeschluss, Standardvertragsklauseln oder eines anderen zulässigen Transfermechanismus.

Standardvertragsklauseln

Soweit erforderlich, gelten die jeweils anwendbaren Standardvertragsklauseln der Europäischen Kommission zwischen den beteiligten Parteien bzw. in der Lieferkette mit Unterauftragsverarbeitern.

Zusätzliche Schutzmaßnahmen

Der Auftragnehmer berücksichtigt, soweit erforderlich und verfügbar, zusätzliche vertragliche, technische und organisatorische Schutzmaßnahmen wie Transportverschlüsselung, Zugriffsbeschränkungen, Datenminimierung und Prüfung behördlicher Zugriffsersuchen.

Informationsbereitstellung

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage angemessene Informationen zu bekannten Drittlandbezügen und eingesetzten Transfermechanismen bereit, soweit keine Geheimhaltungs-, Sicherheits- oder Drittinteressen entgegenstehen.

Änderungen

Wesentliche Änderungen von Transfermechanismen oder Unterauftragsverarbeitern werden nach den Regelungen zu Unterauftragsverarbeitern mitgeteilt.