

AV-Vertrag

Auftragsverarbeitungsvertrag gemaess Art. 28 DSGVO

Status	Entwurf zur rechtlichen Pruefung
Version	1.0
Wirksam ab	2026-07-01
Auftragnehmer	Qourses UG (haftungsbeschraenkt) · vertreten durch den Geschaefsfuehrer Dennis von der Bey
Kunde	Musterkunde GmbH

Auftraggeber

Musterkunde
Musterkunde GmbH
Musterstrasse 1, 10115 Berlin
Vertreten durch: Max Mustermann

Auftragnehmer

Qourses UG (haftungsbeschaenkt)
Qourses UG (haftungsbeschaenkt)
Anschrift gemaess Impressum
Vertreten durch: Dennis von der Bey, Geschaefsfuehrer

Gegenstand und Dauer

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch Qourses UG (haftungsbeschaenkt) als Auftragnehmer fuer den Auftraggeber im Zusammenhang mit der Nutzung der Qourses-Plattform fuer Kursbuchung, Teilnehmerverwaltung, Zahlungs- und Kommunikationsprozesse.

Der Vertrag beginnt am 2026-07-01 und gilt fuer die Dauer des Hauptvertrags ueber die Nutzung von Qourses. Kuendigungs- und Loeschpflichten aus diesem Vertrag bleiben unberuehrt.

Art und Zweck der Verarbeitung

Die Verarbeitung dient der Bereitstellung eines Software-as-a-Service-Angebots fuer Kursanbieter. Qourses verarbeitet personenbezogene Daten nur dokumentiert und weisungsgebunden, soweit dies fuer Betrieb, Wartung, Support, Sicherheit und Vertragserfuellung erforderlich ist.

Weisungen des Auftraggebers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich auf dokumentierte Weisung des Auftraggebers, sofern keine gesetzliche Pflicht zur Verarbeitung besteht. Weisungen koennen im Hauptvertrag, in diesem Vertrag, ueber Administrationsfunktionen der Plattform oder in Textform erteilt werden.

Vertraulichkeit

Der Auftragnehmer verpflichtet alle zur Verarbeitung befugten Personen auf Vertraulichkeit, soweit keine gesetzliche Verschwiegenheitspflicht besteht. Der Zugriff wird auf Personen beschaenkt, die ihn fuer Betrieb, Support oder Wartung benoetigen.

Technische und organisatorische Massnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Massnahmen gemaess 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.

Unterauftragsverarbeiter

Der Auftraggeber genehmigt die in Anlage 3 aufgefuehrten Unterauftragsverarbeiter. Der Auftragnehmer informiert den Auftraggeber ueber beabsichtigte Aenderungen, sodass der Auftraggeber aus wichtigem datenschutzrechtlichem Grund widersprechen kann.

Betroffenenrechte und Mitwirkung

Der Auftragnehmer unterstuetzt den Auftraggeber unter Beruecksichtigung der Art der Verarbeitung angemessen bei der Erfuellung von Betroffenenrechten, Datenschutz-Folgenabschaetzungen, Meldungen von Datenschutzverletzungen und Nachweispflichten.

Loeschung und Rueckgabe

Nach Ende der Leistungserbringung loescht oder gibt der Auftragnehmer personenbezogene Daten nach Wahl des Auftraggebers zurueck, 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, waehrend ueblicher Geschaeftszeiten und unter Wahrung von Sicherheit, Vertraulichkeit und Betriebsstabilitaet.

Schlussbestimmungen

Aenderungen dieses Vertrags beduerfen der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist. Bei Widerspruechen gehen die Regelungen dieses Vertrags den datenschutzbezogenen Regelungen des Hauptvertrags vor.

Ort, Datum, Unterschrift Auftraggeber

Ort, Datum, Unterschrift Auftragnehmer

Anlage 1: Beschreibung der Verarbeitung

Verarbeitungszwecke

Bereitstellung der Qourses-Plattform fuer Kursbuchung, Teilnehmerverwaltung, Kommunikation, Abrechnung, Support, Fehleranalyse und Sicherheit.

Kategorien betroffener Personen

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

Datenkategorien

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

Verarbeitungstaetigkeiten

Erheben, Speichern, Strukturieren, Anzeigen, Uebermitteln, Abgleichen, Einschraenken, Loeschen und Exportieren im Rahmen der Plattformfunktionen.

Anlage 2: Technische und organisatorische Massnahmen

Zugriffskontrolle

Rollen- und berechtigungsbasierter Zugriff, administrative Konten nur fuer berechnigte Personen, starke Authentisierung fuer interne Systeme soweit verfuegbar.

Transport- und Speicherschutz

Verschlüsselte Uebertragung per TLS, getrennte Mandantenlogik, kontrollierte Backups und sichere Konfiguration produktiver Systeme.

Verfuegbarkeit

Betriebsueberwachung, Fehlerprotokollierung, Backup- und Wiederherstellungsprozesse, Schutz vor unbeabsichtigter Zerstoerung oder Verlust.

Verfahren

Dokumentierte Support- und Incident-Prozesse, Vertraulichkeitsverpflichtungen, datenschutzbewusste Entwicklung und regelmässige Ueberpruefung der Massnahmen.

Anlage 3: Unterauftragsverarbeiter

Anbieter	Leistung / Datenkategorien	Ort der Verarbeitung / Hinweise
Fly.io	Hosting der Courses API und Backend-Ausführung; Verkehrs-, Authentifizierungs-, Kurs-, Buchungs-, Zahlungsstatus- und Supportdaten, soweit ueber die API verarbeitet.	Backend-App courses-production; genaue Region und DPA vor Kundennutzung final pruefen.
Crunchy Bridge	Managed PostgreSQL fuer Anwendungsdaten; Organisationen, Nutzer, Kurse, Termine, Buchungen, Bestellungen, Zahlungsreferenzen, Benachrichtigungs- und Audit-/Betriebsdaten.	Produktionscluster auf AWS eu-central-1 laut Infrastrukturkonfiguration.
MongoDB Atlas	Managed MongoDB fuer Hintergrundjobs / Pulse; Job-Metadaten, Zeitplaene und technische Verarbeitungsdaten.	Atlas-Cluster auf AWS EU_CENTRAL_1 laut Infrastrukturkonfiguration.
CloudAMQP	Managed RabbitMQ fuer asynchrone Verarbeitung und Benachrichtigungsqueues; technische Nachrichten zu E-Mail-, Push-, Buchungs- und Plattformereignissen.	AWS eu-central-1 laut Infrastrukturkonfiguration.
Cloudflare	DNS, Reverse Proxy/CDN, Pages Hosting, Images, Turnstile und Realtime-Kit; IP-/Requestdaten, Webseitenaufrufe, hochgeladene Bilder, Captcha-Token, Meeting-/Teilnehmer-Token und ggf. Audio-/Videodaten bei Online-Kursraeumen.	Einsatz fuer qours.es, app.qours.es, API-Proxyed Traffic, Shortlinks, Bilder und optionale Online-Kursraeume. Region/Drittlandtransfer ueber Cloudflare DPA pruefen.
Auth0	Authentifizierung und Identitaetsverwaltung; E-Mail-Adresse, Vorname, Nachname, Login-IDs, Rollen, Berechtigungen, Session- und Token-Metadaten.	Custom Domain auth.qours.es; Auth0 versendet Auth-E-Mails ueber Postmark.
Stripe	Zahlungsabwicklung, Stripe Connect, Checkout, Billing Portal und Webhooks; Organisations- und Zahlungsprofilinformationen, Rechnungs-/Zahlungsdaten, Zahlungsstatus, Stripe-IDs und ggf. Teilnehmer-/Bestellbezug.	Einsatz fuer Courses-Abos und Kurszahlungen; Stripe kann je nach Zahlungsfluss eigenstaendig Verantwortlicher sein. Rechtliche Einordnung final pruefen.
Postmark	Transaktionaler E-Mail-Versand; E-Mail-Adressen, Namen, Buchungs-/Bestell-/Kursinformationen und Auth0-System-E-Mails.	Produktionsserver courses-production; auch als SMTP-Provider fuer Auth0 konfiguriert.
Sentry	Fehleranalyse und Performance-Monitoring fuer Backend, Frontend, Mobile und Shortlinks; technische Fehlerdaten, User-Kontext, IP-/Requestdaten und maskierte Session-Replay-Daten.	Frontend-Replay maskiert Text und Medien; DSNs fuer Produktionsprojekte konfiguriert.
Better Stack / Better Uptime	Logging, Monitoring und Status Page; Backend-, Cloudflare-, Auth0- und Datenbanklogs sowie Uptime-Pruefungen.	Produktionsquellen fuer Backend, Cloudflare, Auth0 und Datenbank konfiguriert. Log-Inhalte und Aufbewahrung final pruefen.

Anbieter	Leistung / Datenkategorien	Ort der Verarbeitung / Hinweise
Google / Firebase Cloud Messaging	Android Push-Benachrichtigungen; Push-Token, technische Geraete-/Installationsdaten und Benachrichtigungsinhalte.	GCP/Firebase-Projekt fuer FCM konfiguriert; Einsatz abhaengig von Mobile-Push-Funktion.
Apple Push Notification service	iOS Push-Benachrichtigungen; Push-Token, technische Geraete-/Installationsdaten und Benachrichtigungsinhalte.	Einsatz abhaengig von Mobile-Push-Funktion.
Google Maps Platform	Ortsauswahl und Ortsreferenzen; eingegebene Such-/Ortsdaten, Place IDs und technische Nutzungsdaten.	API-Key im Frontend konfiguriert; Einsatz bei Standortverwaltung.
Mapbox	Kartendarstellung; Standortkoordinaten, Kartenaufrufe und technische Nutzungsdaten.	Frontend-Kartenkomponente mit Mapbox Access Token konfiguriert.
Crisp	Support-Chat und Identitaetsverifikation; Chat-Inhalte, E-Mail-Adresse bzw. Identifikationshash und technische Supportdaten.	Einsatz auf Courses-Marketing-/Support-Oberflaechen; konkrete Aktivierung fuer App/Support final pruefen.

Anlage 4: Loeschung, Rueckgabe, Audit und Support

Export

Der Auftraggeber kann verfuegbare Plattformexporte nutzen oder einen angemessenen Export in Textform anfordern.

Loeschung

Nach Vertragsende werden produktive personenbezogene Daten nach Ablauf technisch notwendiger Fristen geloescht, soweit keine gesetzlichen Aufbewahrungspflichten bestehen.

Backups

Backups werden im regulaeren Sicherungszyklus ueberschrieben oder geloescht und nur fuer Wiederherstellungszwecke verwendet.

Auditunterstuetzung

Anfragen werden ueber den Supportkanal koordiniert. Vor-Ort-Pruefungen erfordern angemessene Vorlaufzeit und Schutz von Dritt- und Betriebsgeheimnissen.

Aenderungshistorie

Version	Datum	Aenderung
1.0	2026-07-01	Erstfassung des AV-Vertrags fuer Qourses.