Anlage 3: Genehmigte Subunternehmer

> **Info**: Diese Anlage ist Bestandteil der Auftragsverarbeitungsvereinbarung (AVV) und listet alle genehmigten Subunternehmer auf. Die Serverstandorte sind bewusst auf EU/DE-Regionen beschränkt, um DSGVO-Konformität zu gewährleisten. Der Stand des Dokuments und die Subunternehmer-Liste werden regelmäßig auf Aktualität überprüft.

Stand: 29. Juli 2025

Zum Zeitpunkt der Beauftragung genehmigt der Auftraggeber den Einsatz folgender Subunternehmer für die nachfolgend dargestellten Tätigkeiten:

Name/ Firma	**Anschrift**	**Serverstandort(e)**	**Tätigkeit**
Google Cloud EMEA Limited**1	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Ireland	Frankfurt (europe-west3), Belgien (europe-west1)	Hosting von virtuellen Maschinen für Entwicklung, Monitoring und Betriebs-Support, Optional Betrieb von LLM-Modellen (u.a. Anthropic, Gemini und Llama Modelle) über Vertex Ai.
OVH GmbH**2	Oskar-Jäger-Str. 173/ K6, 50825 Köln, Deutschland	Frankfurt (DE), Graveline (FR)	Betrieb der lector.ai Platform-as-a-Service und der LLM-Proxy-Services.
Azure OpenAI Service**3	Microsoft Ireland South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin 18, D18 P521, Ireland	Deutschland (Germany West Central)	Betrieb von DSGVO-konformen GPT-4 und ähnlichen Large Language Models über den Azure OpenAI Service.
n8n GmbH**4	Novalisstr. 10, 10115, Berlin, Germany	Frankfurt (DE)	Optional: Betrieb der n8n-Workflow-Automatisierungsplattform für die Integration von Geschäftsprozessen und Datenflüssen.

Name/ Firma	Anschrift	Serverstandort(e)	Tätigkeit
HubSpot Ireland Limited**5	One Dockland Central, Guild Street, Dublin 1, Ireland	Frankfurt (EU Central)	CRM-System, Kundenkommunikation, Marketing E-Mails und Verwaltung von Kundenbeziehungen.
Stripe Payments Europe Ltd.**6	The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland	Europa (EU-Region, Dublin)	Abrechnung und Zahlungsabwicklung für die Dienste von lector.ai.

1. Die Auftragsverarbeitung durch den Subunternehmer Google LLC wird durch das Data Processing Agreement https://cloud.google.com/terms/data-processing-terms geregelt und fällt unter die Standard-Datenschutz-Klauseln (SDK) https://cloud.google.com/terms/sccs/eu-c2p. Zusätzlich ist Google Cloud seit Oktober 2023 nach dem EU-US Data Privacy Framework zertifiziert, was einen weiteren Rechtsrahmen für den Datentransfer zwischen der EU und den USA bietet.

   Für die Nutzung der Google Cloud Vertex AI gelten die Zusatzbedingungen der Gemini API (https://ai.google.dev/gemini-api/terms?hl=de). Für diese kostenpflichtigen Dienste gilt insbesondere: „Wenn Sie kostenpflichtige Dienste nutzen, verwendet Google Ihre Prompts (einschließlich zugehöriger Systemanweisungen, im Cache gespeicherter Inhalte und Dateien wie Bilder, Videos oder Dokumente) oder Antworten nicht, um die Produkte von Google zu verbessern, und verarbeitet Ihre Prompts und Antworten in Übereinstimmung mit dem Zusatz zur Datenverarbeitung für Produkte, bei denen Google ein Datenauftragsverarbeiter ist (Google Data Processing Addendum for Products Where Google is a Data Processor). Diese Daten können in jedem Land, in dem Google oder seine Vertreter Einrichtungen unterhalten, vorübergehend oder im Cache gespeichert werden."

   Google Cloud verschlüsselt die Daten standardmäßig serverseitig, bevor sie auf ein Laufwerk geschrieben werden. Bei der Übertragung von und zum Server findet TLS-Verschlüsselung statt, inaktive Daten werden seitens des Cloud Anbieters via AES256 verschlüsselt. Das Verschlüsselungsschlüsselmanagement wird von lector.ai verwaltet (Cloud Key Management Service).

   Google ist nach ISO27018 zertifiziert und wird jährlich auditiert. Weitere Informationen finden Sie unter: https://cloud.google.com/security/compliance/iso-27018?hl=de Zertifikate können über den Compliance Reports Manager heruntergeladen werden: https://cloud.google.com/security/compliance/compliance-reports-manager#/ReportType=Certificate&ProductArea=Google_Cloud

   Lector.ai bietet über Google Vertex Ai verschiedene LLM Modelle an, die ausschließlich auf Servern innerhalb der Europäischen Union betrieben werden. Auf der Plattform ist eindeutig gekennzeichnet, wo die jeweils ausgewählten Modelle betrieben werden. Es liegt in der Wahl des Kunden, welche Modelle und EU-Standorte gewählt werden.

2. Die Auftragsverarbeitung durch den Subunternehmer OVH GmbH wird durch das Data Processing Agreement https://us.ovhcloud.com/legal/data-processing-agreement/ geregelt.

   Lector.ai bleibt alleiniger Eigentümer der von ihm im Rahmen der OVH Dienstleistungen gespeicherten Daten. OVH greift weder auf diese Daten zu noch werden sie verwendet, solange dies nicht für die korrekte Ausführung der Dienstleistungen notwendig ist, und auch dann nur innerhalb der technischen Grenzen dieser Dienstleistungen. OVH ist es untersagt, die genannten Daten weiterzuverkaufen oder für eigene Zwecke (zum Beispiel Datamining, Profiling oder Direktmarketing) zu verwenden.

   OVH ist nach ISO 27001, ISO 27017 und ISO 27018 zertifiziert. Weitere Informationen finden Sie unter: https://www.ovhcloud.com/de/compliance/iso-27001-27017-27018/

3. Im Fall von OpenAI API-Diensten (wie dem Microsoft Azure OpenAI Service), werden keine Daten für das Training von Modellen oder für andere Zwecke von OpenAI verwendet, es sei denn, es wurde ausdrücklich eine Erlaubnis dazu erteilt. Bei der Nutzung über Azure wird die Datenverarbeitung durch Microsofts Datenschutzrichtlinien (s. Microsoft DPA in Anhang 2) geregelt. Microsoft speichert und verarbeitet die Daten nicht für eigene Zwecke und sichert zu, dass die Kundendaten vertraulich behandelt werden.

   Quelle: https://learn.microsoft.com/de-de/legal/cognitive-services/openai/data-privacy (Stand: 23. September 2024)

   Wichtige Datenschutzaspekte des Azure OpenAI Service:

   - Alle Daten werden ausschließlich in der EU-Region (Germany West Central) verarbeitet
   - Microsoft implementiert strenge Zugriffskontrollen und Protokollierung für Systemadministratoren
   - Automatische Verschlüsselung der Daten im Ruhezustand (Storage) und während der Übertragung (TLS 1.2)
   - Keine Speicherung von Prompts oder Antworten nach Abschluss der Verarbeitung
   - Konformität mit ISO 27001, SOC 1/2/3, und DSGVO-Anforderungen
   - Microsoft bietet standardmäßig Customer Managed Keys (CMK) für zusätzliche Kontrolle
   - Regelmäßige Sicherheitsaudits und Penetrationstests durch unabhängige Dritte
   - Transparente Incident Response und Breach Notification Prozesse gemäß DSGVO

4. Die Auftragsverarbeitung durch den optionalen Subunternehmer n8n GmbH wird durch das Data Processing Agreement https://n8n.io/legal/#data geregelt. Die n8n GmbH ist ein in Deutschland ansässiges Unternehmen, das eine Workflow-Automatisierungsplattform bereitstellt. Sämtliche Datenverarbeitung findet in der EU statt, speziell im Rechenzentrum in Frankfurt.

   Die n8n-Plattform kann optional zur Automatisierung von Geschäftsprozessen und zur Integration verschiedener Systeme eingesetzt werden. Die Daten werden während der Übertragung mittels TLS 1.2/1.3 und im Ruhezustand mittels AES-256 verschlüsselt. n8n ist nach ISO 27001 zertifiziert und wird regelmäßig auf Sicherheitsstandards überprüft.

   Die Nutzung der n8n-Plattform ist optional und erfolgt nur nach expliziter Beauftragung durch den Kunden.

5. Die Auftragsverarbeitung durch den Subunternehmer HubSpot Ireland Limited wird durch das Data Processing Agreement https://legal.hubspot.com/dpa geregelt. HubSpot ist nach ISO 27001, SOC 2 Typ II und verschiedenen anderen Sicherheitsstandards zertifiziert.

   HubSpot wird für die Verwaltung von Kundenbeziehungen (CRM), für Marketing-E-Mails und für die Kommunikation mit Kunden eingesetzt. Die Datenverarbeitung findet ausschließlich in der EU statt (Rechenzentrum in Frankfurt).

   Die Daten werden während der Übertragung mit TLS 1.2 und im Ruhezustand mit AES-256 verschlüsselt. HubSpot bietet umfangreiche Kontrollen zum Schutz personenbezogener Daten gemäß DSGVO und stellt entsprechende Funktionen zur Erfüllung von Betroffenenrechten bereit.

   Die HubSpot-Plattform respektiert die EU-Standardvertragsklauseln (SCCs) und ermöglicht die Löschung oder Anonymisierung von Kundendaten gemäß den geltenden Datenschutzbestimmungen.

6. Die Auftragsverarbeitung durch den Subunternehmer Stripe Payments Europe Ltd. wird durch das Data Processing Agreement https://stripe.com/de/legal/dpa geregelt. Stripe ist nach PCI DSS Level 1, ISO 27001, SOC 1 Typ II und SOC 2 Typ II zertifiziert.

   Stripe wird für die Abrechnung und Zahlungsabwicklung der lector.ai-Dienste eingesetzt. Die Datenverarbeitung erfolgt in der EU-Region (Dublin). Stripe implementiert branchenführende Sicherheitsmaßnahmen zum Schutz von Zahlungsdaten und personenbezogenen Daten.

   Die Daten werden während der Übertragung mit TLS 1.2+ und im Ruhezustand mit AES-256 verschlüsselt. Stripe erfüllt alle Anforderungen der DSGVO und stellt Tools zur Verfügung, um Betroffenenrechte zu gewährleisten.

   Stripe behandelt alle Daten vertraulich und verwendet sie ausschließlich zur Bereitstellung der Zahlungsdienste, ohne sie für eigene Zwecke zu nutzen oder weiterzuverkaufen.