Auftragsverarbeitungsvertrag
gemäß Art. 28 DSGVO

zwischen

dem jeweiligen Kunden, der die Plattform EHRENBEHÖRDE nutzt und sich hierfür registriert

- nachfolgend "Verantwortlicher" -

und

Griffin & Kale GmbH
(Marke: EHRENBEHÖRDE)
Beverbäker Wiesen 6b
26123 Oldenburg
vertreten durch die Geschäftsführer: Peter Gneuß, Nicole Gneuß
HRB 219182, Amtsgericht Oldenburg
USt-IdNr.: DE358951231

- nachfolgend "Auftragsverarbeiter" -

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen zum Zweck der Bereitstellung und des Betriebs der Plattform EHRENBEHÖRDE einschließlich der darüber angebotenen Leistungen (insbesondere KI-Pflichtschulungen). Art und Zweck der Verarbeitung ergeben sich aus diesem Vertrag.

(2) Die Vertragslaufzeit entspricht der Laufzeit des zugrundeliegenden Leistungsvertrages.

(3) Dieser Vertrag kommt dadurch zustande, dass sich der Verantwortliche für die Nutzung der Plattform registriert und diesen Auftragsverarbeitungsvertrag im Rahmen des Registrierungs- bzw. Bestellvorgangs in elektronischer Form akzeptiert. Eine eigenhändige Unterzeichnung ist gemäß Art. 28 Abs. 9 DSGVO nicht erforderlich. Identität und Anschrift des Verantwortlichen ergeben sich aus den bei der Registrierung angegebenen Daten.

§ 2 Art und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten für folgende Zwecke:

Art der Verarbeitung	Beschreibung
Zweck	Bereitstellung und Betrieb der Plattform EHRENBEHÖRDE einschließlich der darüber angebotenen Leistungen (insbesondere KI-Pflichtschulungen, Lerninhalte sowie Konto- und Kursverwaltung)
Datenarten	Konto-/Bestandsdaten (z. B. E-Mail-Adresse, ggf. Name), Nutzungsdaten (z. B. Kursfortschritt, Aktivitäts-/Log-Daten)
Betroffene Personen	Nutzer der Plattform, insbesondere Mitarbeitende des Verantwortlichen, die die Plattform nutzen bzw. an Schulungen teilnehmen

§ 3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur im Rahmen der dokumentierten Weisungen des Verantwortlichen, es sei denn, er ist durch Unionsrecht oder das Recht der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet.

(2) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten gemäß Art. 32 bis 36 DSGVO, soweit dies möglich ist.

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die konkreten Maßnahmen sind in Anlage 1 (TOM-Katalog) zu diesem Vertrag detailliert beschrieben.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter ist berechtigt, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Verantwortlichen unverzüglich mitzuteilen.

5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Beauftragung folgender Unterauftragsverarbeiter:

Unterauftrags-verarbeiter	Zweck	Standort	Garantien
Memberspot GmbH	Lernplattform und Kursverwaltung	Deutschland (EU)	AVV, EU-DSGVO
ActiveCampaign LLC	E-Mail-Marketing und Automatisierung	EU (Frankfurt), USA	SCC, TIA, EU-Hosting

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vor geplanten Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern in Textform (E-Mail ausreichend). Der Verantwortliche kann gegen diese Änderungen innerhalb von 30 Tagen nach Zugang der Information Widerspruch einlegen.

(3) Der Auftragsverarbeiter stellt sicher, dass die Unterauftragsverarbeiter die gleichen Datenschutzpflichten erfüllen wie in diesem Vertrag festgelegt. Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der dem vorliegenden Auftragsverarbeitungsvertrag inhaltlich gleichwertig ist.

(4) Soweit Daten durch Unterauftragsverarbeiter außerhalb der EU/EWR verarbeitet werden, gelten die Regelungen des § 10 dieses Vertrages.

§ 6 Rechte betroffener Personen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte betroffener Personen.

(2) Der Auftragsverarbeiter leitet Anfragen betroffener Personen unverzüglich, spätestens innerhalb von 2 Werktagen, an den Verantwortlichen weiter.

§ 7 Löschung und Rückgabe von Daten

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht oder übergibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten, die im Zusammenhang mit der Auftragsverarbeitung stehen, es sei denn, das Unionsrecht oder das Recht eines Mitgliedstaats sieht eine Verpflichtung zur Speicherung der personenbezogenen Daten vor.

(2) Die Löschung oder Rückgabe erfolgt innerhalb von 60 Tagen nach Vertragsende, sofern keine abweichende Weisung des Verantwortlichen vorliegt.

(3) Der Auftragsverarbeiter bestätigt die vollständige Löschung oder Rückgabe in Textform (E-Mail ausreichend) gegenüber dem Verantwortlichen.

§ 8 Kontroll- und Prüfrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

(2) Der Auftragsverarbeiter ermöglicht dem Verantwortlichen oder einem von diesem beauftragten Prüfer Inspektionen und Überprüfungen. Diese sind:

a) mindestens 14 Tage im Voraus anzukündigen,

b) auf maximal einmal jährlich beschränkt (außer bei begründetem Verdacht auf Datenschutzverstöße oder bei Aufforderung durch Aufsichtsbehörden),

c) während der üblichen Geschäftszeiten durchzuführen,

d) so durchzuführen, dass der laufende Betrieb nicht unverhältnismäßig gestört wird.

(3) Die Kosten für Inspektionen trägt der Verantwortliche, sofern nicht ein Verstoß gegen diesen Vertrag durch den Auftragsverarbeiter festgestellt wird.

§ 9 Meldepflicht bei Datenpannen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und bei der Benachrichtigung betroffener Personen gemäß Art. 33 und 34 DSGVO.

(2) Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, an den Verantwortlichen. Die Meldung enthält mindestens:

a) Beschreibung der Art der Verletzung,

b) Kategorien und ungefähre Anzahl betroffener Personen und Datensätze,

c) wahrscheinliche Folgen der Verletzung,

d) ergriffene oder vorgeschlagene Maßnahmen zur Behebung.

§ 10 Datenübermittlung in Drittländer

(1) Die Verarbeitung der personenbezogenen Daten erfolgt vorrangig in der Europäischen Union bzw. im Europäischen Wirtschaftsraum.

(2) Soweit Unterauftragsverarbeiter Daten in Drittländern verarbeiten (insbesondere ActiveCampaign LLC mit Zugriffsmöglichkeit aus den USA), gelten folgende Garantien:

a) Es werden EU-Standardvertragsklauseln (SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO abgeschlossen,

b) Der Auftragsverarbeiter hat ein Transfer Impact Assessment (TIA) durchgeführt und dokumentiert,

c) Die Daten werden vorrangig auf EU-Servern gehostet (ActiveCampaign: Frankfurt),

d) Technische Maßnahmen (Verschlüsselung, Pseudonymisierung) minimieren Risiken bei möglichen Zugriffen durch US-Behörden.

(3) Der Verantwortliche wurde über potenzielle Risiken durch Drittlandübermittlungen (insbesondere US Cloud Act, FISA 702) informiert und akzeptiert diese im Rahmen der getroffenen Garantien.

§ 11 Datenschutz-Folgenabschätzung und Vorabkonsultation

Der Auftragsverarbeiter unterstützt den Verantwortlichen, soweit erforderlich, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO sowie bei einer eventuell notwendigen Vorabkonsultation bei der Aufsichtsbehörde gemäß Art. 36 DSGVO.

§ 12 Datenschutzbeauftragte

Soweit bei einer Partei ein Datenschutzbeauftragter benannt ist, sind dessen Kontaktdaten der anderen Partei mitzuteilen. Änderungen sind unverzüglich zu kommunizieren.

§ 13 Dokumentationspflichten

(1) Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

(2) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage Auszüge aus dem Verzeichnis zur Verfügung, soweit diese die gegenständliche Auftragsverarbeitung betreffen.

§ 14 Weisungsbefugnis

(1) Weisungen werden initial durch diesen Vertrag erteilt. Einzelweisungen können in Textform (E-Mail ausreichend) durch den Verantwortlichen erteilt werden.

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

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung bis zur Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

§ 15 Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, sowie den Regelungen des zugrundeliegenden Leistungsvertrages.

§ 16 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien verpflichten sich, eine unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

Anlagen

Dieser Vertrag wird ergänzt durch:

Anlage 1: Technische und organisatorische Maßnahmen (TOM-Katalog)

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Verantwortlicher (Name gemäß Registrierungsdaten)	**Auftragsverarbeiter** Griffin & Kale GmbH

Anlage 1

Technische und organisatorische Maßnahmen

(TOM-Katalog gem. Art. 32 DSGVO)

zum Auftragsverarbeitungsvertrag zwischen dem Verantwortlichen und der Griffin & Kale GmbH

Vorbemerkung:

Die Griffin & Kale GmbH setzt für die Erbringung der Dienstleistung spezialisierte Unterauftragsverarbeiter ein (Memberspot und ActiveCampaign). Die technische Infrastruktur (Rechenzentren, Server, Backups etc.) wird vollständig durch diese Unterauftragsverarbeiter bereitgestellt und betrieben. Die nachfolgenden Maßnahmen beschreiben die von Griffin & Kale GmbH selbst umgesetzten organisatorischen Maßnahmen sowie die vertraglich mit den Unterauftragsverarbeitern vereinbarten technischen Garantien.

1. Organisatorische Maßnahmen der Griffin & Kale GmbH

1.1 Zugangskontrolle zu Verwaltungssystemen

- Individuelle Benutzerkonten für jeden Mitarbeiter mit persönlichen Zugangsdaten
- Nutzung starker Passwörter (mind. 12 Zeichen, Kombination aus Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen)
- Zwei-Faktor-Authentifizierung (2FA) für den Zugriff auf Memberspot und ActiveCampaign
- Sofortige Deaktivierung von Zugängen bei Ausscheiden von Mitarbeitern

1.2 Zugriffskontrolle und Berechtigungsmanagement

- Prinzip der minimalen Rechtevergabe: Mitarbeiter erhalten nur Zugriff auf die für ihre Tätigkeit notwendigen Daten und Funktionen
- Regelmäßige Überprüfung der Berechtigungen (mindestens jährlich)
- Dokumentation, welcher Mitarbeiter Zugriff auf welche Systeme hat

1.3 Vertraulichkeitsverpflichtung

- Alle Mitarbeiter sind vertraglich auf Vertraulichkeit und Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter für Datenschutzthemen

1.4 Auswahl und Kontrolle von Unterauftragsverarbeitern

- Sorgfältige Auswahl von Unterauftragsverarbeitern nach Datenschutz- und Sicherheitskriterien
- Abschluss von Auftragsverarbeitungsverträgen mit allen Unterauftragsverarbeitern
- Regelmäßige Überprüfung der Sicherheitsstandards der Unterauftragsverarbeiter

1.5 Datenschutz-Management

- Jährliche Überprüfung und Aktualisierung dieser technischen und organisatorischen Maßnahmen
- Dokumentierte Prozesse für den Umgang mit Betroffenenanfragen
- Incident-Response-Prozess: Bei Kenntnis von Datenpannen erfolgt unverzügliche Meldung an den Verantwortlichen (innerhalb 24 Stunden)

1.6 Datenminimierung und Löschkonzept

- Erhebung nur der für die Plattformnutzung notwendigen Daten (z. B. E-Mail-Adresse, Kursfortschritt, Nutzungsdaten)
- Keine Erhebung von Namen oder weiteren personenbezogenen Daten, sofern nicht vom Verantwortlichen ausdrücklich gewünscht
- Dokumentiertes Löschkonzept: Daten werden nach Vertragsende oder auf Weisung gelöscht

2. Technische Maßnahmen der Unterauftragsverarbeiter

Die folgenden technischen Maßnahmen werden durch die Unterauftragsverarbeiter bereitgestellt und sind in deren Auftragsverarbeitungsverträgen und Sicherheitsdokumentationen beschrieben:

2.1 Memberspot GmbH (Lernplattform)

- Hosting in zertifizierten deutschen Rechenzentren
- Verschlüsselte Datenübertragung (TLS/SSL)
- Tägliche Backups
- Firewall und DDoS-Schutz
- Rollenbasierte Zugriffskontrolle innerhalb der Plattform

2.2 ActiveCampaign LLC (E-Mail-Marketing)

- Datenhosting auf EU-Servern (Frankfurt, Deutschland)
- Verschlüsselte Datenübertragung (TLS 1.2 oder höher)
- ISO 27001 zertifizierte Rechenzentren

- Regelmäßige Sicherheitsaudits und Penetrationstests
- Standardvertragsklauseln (SCC) für eventuelle Drittlandübermittlungen

3. Gemeinsame Sicherheitsstandards

Alle eingesetzten Unterauftragsverarbeiter erfüllen folgende Mindeststandards:

- Verschlüsselte Datenübertragung (mindestens TLS 1.2)
- Regelmäßige Sicherheitsupdates und Patch-Management
- Monitoring und Incident-Response-Prozesse
- Physische Sicherheit der Rechenzentren (Zutrittskontrolle, Videoüberwachung)
- Backup- und Wiederherstellungsverfahren

4. Nachweispflichten und Transparenz

Griffin & Kale GmbH stellt auf Anfrage folgende Nachweise zur Verfügung:

- Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern
- Sicherheitsdokumentationen der Unterauftragsverarbeiter
- Zertifikate (sofern vorhanden, z.B. ISO 27001)
- Dokumentation der eigenen organisatorischen Maßnahmen

Aktualisierung und Anpassung:

Diese technischen und organisatorischen Maßnahmen werden mindestens jährlich überprüft und bei Bedarf an den Stand der Technik sowie an geänderte Anforderungen angepasst. Wesentliche Änderungen werden dem Verantwortlichen unverzüglich mitgeteilt.