DIGITALE Vergabe

Kritera UG (haftungsbeschränkt)
Gustav-Herbster-Straße 8, 65307 Bad Schwalbach
info@digitale-vergabe.de · digitale-vergabe.de

Vertrag zur Auftragsverarbeitung

Nach Art. 28 DSGVO, Anlage zu den Allgemeinen Geschäftsbedingungen für Digitale-Vergabe.DE. Stand: November 2026.

zwischen dem Kunden (Verantwortlicher, nachfolgend „Auftraggeber“)

und der Kritera Unternehmergesellschaft (haftungsbeschränkt), Gustav-Herbster-Straße 8, 65307 Bad Schwalbach, HRB 36663, Amtsgericht Wiesbaden (Auftragsverarbeiter, nachfolgend „Auftragnehmer“)

Dieser Vertrag ist Anlage zu den Allgemeinen Geschäftsbedingungen für Digitale-Vergabe.DE und kommt mit dem Hauptvertrag zustande. Auf Wunsch stellt der Auftragnehmer ihn auch als unterschriebenes Exemplar bereit.

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber die Software Digitale-Vergabe.DE als Dienst bereit (Hauptvertrag: Angebot oder Bestellung samt AGB für Digitale-Vergabe.DE). Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag regelt die Rechte und Pflichten beider Seiten dazu.

(2) Der Vertrag gilt für die Laufzeit des Hauptvertrags und darüber hinaus, solange der Auftragnehmer Daten des Auftraggebers verarbeitet (insbesondere bis zur Löschung nach § 11).

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art und Zweck: Bereitstellung, Betrieb, Wartung und Support der Software Digitale-Vergabe.DE, insbesondere Speicherung von Verfahrensakten und Unterlagen, Bieterkommunikation, Vertragsverwaltung, Ausführung von KI-Funktionen auf Anforderung der Nutzer, Versand von System-Mails, Betrieb der öffentlichen Verfahrensseiten (Vergabeunterlagen, Registrierung von Unternehmen, Unternehmenskonten) und Übermittlung von Bekanntmachungen an den Vermittlungsdienst des Datenservice Öffentlicher Einkauf auf Weisung des Auftraggebers.

(2) Arten der Daten und Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(3) Die Verarbeitung findet in Deutschland statt. Eine Übermittlung in Drittländer erfolgt nur nach § 7.

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch Unionsrecht oder deutsches Recht zur Verarbeitung verpflichtet; in diesem Fall teilt er dies vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Weisungen sind der Hauptvertrag, dieser Vertrag und die Nutzung der Software durch den Auftraggeber und seine Nutzer (zum Beispiel das Anlegen, Ändern und Löschen von Daten, das Starten einer KI-Funktion oder der Ausschluss einzelner KI-Anbieter durch die Leitung des Hauses). Weitere Weisungen erteilt der Auftraggeber in Textform.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

§ 4 Vertraulichkeit

Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen und die mit den Bestimmungen des Datenschutzes vertraut gemacht wurden.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die Maßnahmen nach Art. 32 DSGVO, die in **Anlage 2** beschrieben sind.

(2) Er darf die Maßnahmen weiterentwickeln, wenn das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt er mit.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber genehmigt die in **Anlage 3** genannten Unterauftragsverarbeiter.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen vor dem Einsatz eines neuen oder dem Wechsel eines Unterauftragsverarbeiters in Textform. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, kann der Auftraggeber den Hauptvertrag zum Zeitpunkt des Wechsels kündigen.

(3) Der Auftragnehmer legt Unterauftragsverarbeitern vertraglich dieselben Datenschutzpflichten auf, die dieser Vertrag ihm auferlegt.

(4) Für KI-Funktionen setzt der Auftragnehmer Mistral AI und, falls gewünscht, Anthropic oder OpenAI ein. Voreingestellt ist derzeit Anthropic (Claude); ein Nutzer kann in der Anwendung einen anderen Anbieter wählen. Für die Sprachfunktionen (Spracheingabe, Sprachgespräch mit dem Vergabe-Nerd und Vorlesen) setzt der Auftragnehmer die Spracherkennung und Sprachausgabe der Mistral AI ein; ein Diktat in Formularen übernimmt die OpenAI Ireland Ltd., wenn das Haus Mistral AI ausgeschlossen und OpenAI zugelassen hat. Die Leitung eines Hauses kann einzelne KI-Anbieter für ihr Haus ausschließen oder den EU-Modus einschalten, in dem die KI-Funktionen über Mistral AI laufen.

§ 7 Übermittlung in Drittländer

(1) Eine Übermittlung in ein Land außerhalb der EU und des EWR erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Das betrifft derzeit die Anthropic PBC (USA) für KI-Funktionen und die Brave Software Inc. (USA) für ergänzende Websuchen. Wählt ein Nutzer OpenAI, kann die OpenAI Ireland Ltd. Daten an verbundene Unternehmen in den USA übermitteln. Mistral AI verarbeitet die Daten in der EU. Grundlage der Übermittlungen in die USA sind das EU-US Data Privacy Framework, soweit der Empfänger zertifiziert ist, und andernfalls die Standardvertragsklauseln der EU-Kommission.

(3) Übermittelt werden nur die Eingaben, die ein Nutzer der jeweiligen Funktion gibt, und die Auszüge aus Unterlagen, die für die angefragte Aufgabe nötig sind. Für Websuchen werden nur Suchbegriffe übermittelt.

§ 8 Rechte der betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anfragen betroffener Personen (Art. 12 bis 22 DSGVO). Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter.

§ 9 Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei den Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzung und vorheriger Konsultation.

§ 10 Meldung von Verletzungen

Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar. Er ergreift unverzüglich Maßnahmen zur Eindämmung und informiert über den Stand.

§ 11 Löschung und Rückgabe

(1) Nach Ende des Hauptvertrags kann der Auftraggeber seine Daten 30 Tage lang exportieren. Danach löscht der Auftragnehmer alle Daten des Auftraggebers innerhalb weiterer 30 Tage, soweit keine gesetzliche Pflicht zur Speicherung besteht. Daten in Datensicherungen werden mit dem regulären Ablauf der Sicherungen gelöscht, spätestens nach sechs Wochen.

(2) Der Auftragnehmer bestätigt die Löschung auf Verlangen in Textform.

§ 12 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Pflichten nach Art. 28 DSGVO nötig sind.

(2) Der Auftraggeber kann Kontrollen nach rechtzeitiger Anmeldung (in der Regel vier Wochen) während der Geschäftszeiten durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Der Nachweis kann auch durch aktuelle Zertifikate oder Prüfberichte der Unterauftragsverarbeiter (zum Beispiel ISO/IEC 27001 des Rechenzentrums) erbracht werden.

§ 13 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.

§ 14 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag in Fragen des Datenschutzes vor.

(2) Änderungen bedürfen der Textform.

(3) Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1: Daten und betroffene Personen

Kategorie betroffener Personen	Arten der Daten
Beschäftigte des Auftraggebers (Bearbeiter, Mitwirkende, Leitung)	Name, dienstliche E-Mail-Adresse, Rolle, Organisation, Anmeldedaten (Passwort nur als Hashwert), bei SSO die Kennung des Identitätsanbieters, Protokolldaten (Zeitpunkt, Aktion, IP-Adresse), Eingaben in KI-Funktionen, Verbrauch von Vergabe-Token (nur für die Person selbst und als Summe für die Verwalter sichtbar), bei der Übermittlung an den Datenservice die E-Mail-Adresse der auslösenden Person
Bieter und ihre Beschäftigten	Name, Unternehmen, E-Mail-Adresse, Telefonnummer, Daten für den zweiten Faktor, Fragen und Nachrichten, Angebote mit Anlagen (können Referenzen, Qualifikationen und Lebensläufe von Personal enthalten), Protokolldaten, bei einem Bieterkonto gespeicherte Suchkriterien
Gäste	Name, E-Mail-Adresse, Freigaben, Protokolldaten
Dritte in Unterlagen	Personenbezogene Angaben, die in Unterlagen des Auftraggebers enthalten sind (zum Beispiel Ansprechpartner)

Besondere Kategorien nach Art. 9 DSGVO sind nicht Gegenstand der Verarbeitung. Der Auftraggeber stellt sicher, dass er solche Daten nicht ohne gesonderte Vereinbarung einbringt.

Anlage 2: Technische und organisatorische Maßnahmen

Bereich	Maßnahmen
Zutritt	Server im Rechenzentrum der Hetzner Online GmbH in Nürnberg. Zutrittskontrolle durch Hetzner nach dessen Zertifizierung (ISO/IEC 27001). Keine Server in eigenen Räumen
Zugang	Anmeldung mit persönlichem Konto, Passwörter nur als Hashwert, optional Single Sign-on des Auftraggebers, zweiter Faktor für Bieter. Administrativer Serverzugang nur über SSH-Schlüssel durch den Geschäftsführer; Anmeldung per Passwort ist deaktiviert, root nur mit Schlüssel
Zugriff	Mandantentrennung je Organisation, Rollen und Freigabeketten, Bieter sehen nur die für sie freigegebenen Verfahren, Verwalter sehen beim Token-Verbrauch nur Summen
Weitergabe	Übertragung ausschließlich verschlüsselt per TLS (Zertifikate von Let's Encrypt). Sicherheitsheader und strenge Content-Security-Policy auf allen Seiten. Angebotseingang: Jede Datei wird beim Hochladen mit AES-256-GCM verschlüsselt, der Schlüssel je Angebot wird aus einem Serverschlüssel, dem Verfahren und einem Zufallswert abgeleitet (scrypt) und nicht im Klartext gespeichert. Vor Ablauf der Angebotsfrist entschlüsselt der Server nicht, auch nicht für den Auftraggeber (Submissionssperre); jeder Versuch wird protokolliert. Die Öffnung erfordert zwei verschiedene Konten (Vieraugenprinzip). Prüfsumme (SHA-256) und Eingangszeit vom Server sichern die Unveränderlichkeit. Keine Ende-zu-Ende-Verschlüsselung: Der Server sieht die Datei im Moment des Hochladens
Eingabe	Ereignisprotokoll in der Anwendung (wer, wann, welche Aktion), Begrenzung von Anfragen je Zeitraum (Rate Limiting)
Verfügbarkeit	Datensicherung von Montag bis Samstag (Datenbank und Dateien der Kunden, 30 Tage aufbewahrt) und wöchentlich (5 Stände), jeweils mit GPG verschlüsselt; Kopie auf einer Storage Box der Hetzner Online GmbH an einem anderen Standort als der Server; wöchentlicher Wiederherstellungstest der jüngsten Sicherung vom Server und von der Storage Box; Überwachung der Erreichbarkeit. Laufende Wartung und Aktualisierung erfolgen in einem nächtlichen Wartungsfenster zwischen 02:00 und 03:00 Uhr (deutsche Zeit), um die Beeinträchtigung der Verfügbarkeit und laufender Verfahren gering zu halten
Trennung	Getrennte Bereiche je Organisation in der Datenbank; im Verbund getrennte Bereiche je Haus
KI-Funktionen	Übermittlung nur der für die Aufgabe nötigen Eingaben und Auszüge, Nutzung der kommerziellen Programmierschnittstellen, deren Bedingungen ein Training mit Kundendaten ausschließen, Ausschluss einzelner Anbieter je Haus möglich
Organisation	Verpflichtung auf Vertraulichkeit, schriftliches Verfahren für Datenschutzvorfälle mit Meldung nach § 10
Wartung	Die Wartung und Weiterentwicklung erfolgt durch den Geschäftsführer, auch mit KI-gestützten Entwicklungswerkzeugen der Anthropic PBC. Abfragen auf Inhaltsdaten des Auftraggebers werden dabei auf das für die Fehlerbehebung Nötige beschränkt; Anthropic ist in Anlage 3 auch für diesen Zweck genannt

Anlage 3: Unterauftragsverarbeiter

Unternehmen	Sitz	Leistung	Grundlage
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Hosting von Website und Anwendung, Rechenzentrum Nürnberg	Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO
Mistral AI SAS	Paris, Frankreich	KI-Funktionen, wählbar und im EU-Modus des Hauses gesetzt; Spracherkennung und Sprachausgabe der Sprachfunktionen	Data Processing Agreement des Anbieters

Unternehmen	Sitz	Leistung	Grundlage
Anthropic PBC	San Francisco, USA	KI-Funktionen (Claude-API), falls gewünscht, derzeit voreingestellt, und KI-gestützte Entwicklungswerkzeuge für Wartung und Weiterentwicklung	Data Processing Addendum, Drittlandübermittlung nach § 7
OpenAI Ireland Ltd.	Dublin, Irland	KI-Funktionen, falls gewünscht (nur wenn vom Nutzer gewählt); Diktat in Formularen, wenn Mistral AI im Haus ausgeschlossen ist	Vertrag zur Auftragsverarbeitung, Drittlandübermittlung nach § 7
Brave Software Inc.	USA	Ergänzende Websuche (nur Suchbegriffe)	Datenverarbeitungsbedingungen des Anbieters, Drittlandübermittlung nach § 7
Microsoft Ireland Operations Ltd.	Dublin, Irland	Versand und Empfang von E-Mails über Microsoft 365	Datenschutznachtrag zu den Microsoft-Produktbedingungen

PayPal (Europe) S.à r.l. et Cie, S.C.A. ist kein Unterauftragsverarbeiter, sondern bei Zahlungen eigener Verantwortlicher.

Der Datenservice Öffentlicher Einkauf (Beschaffungsamt des BMI) und das Amt für Veröffentlichungen der Europäischen Union (TED) sind keine Unterauftragsverarbeiter. Sie sind Empfänger, an die der Auftraggeber Bekanntmachungen übermitteln lässt. Die Übermittlung erfolgt ausschließlich auf ausdrückliche Weisung des Auftraggebers, die eine berechtigte Person durch Bestätigung im System erteilt.

Stand: Oktober 2026