

Vertrag zur Auftragsverarbeitung (AVV) – Herta

gemäß Art. 28 DSGVO · Version 1.0 · Stand: Oktober 2026

zwischen

[**Auftraggeber / Unternehmen**], [Straße Hausnummer], [PLZ Ort] – nachfolgend „Auftraggeber“ –
und

Möhle und Braker Datentechnik GbR, Bahnhofstraße 24, 24647 Wasbek, vertreten durch die
Gesellschafter Rainer Braker und Michael Möhle – nachfolgend „Auftragnehmer“ –

§ 1 Gegenstand und Dauer

- (1) Der Auftragnehmer stellt dem Auftraggeber die webbasierte Software „Herta – HR Tools and Assistants“ (nachfolgend „Herta“) als Software-as-a-Service bereit. Die Einzelheiten der Leistung ergeben sich aus dem Hauptvertrag, bestehend aus der Bestellung des Auftraggebers und den Allgemeinen Geschäftsbedingungen für Herta (nachfolgend „Hauptvertrag“).
- (2) Bei der Erbringung der Leistungen verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien.
- (3) Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Die Pflichten nach § 12 gelten über das Vertragsende hinaus.

§ 2 Art, Zweck und Umfang der Verarbeitung

- (1) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus **Anlage 1**. Sie richten sich nach den vom Auftraggeber gebuchten Modulen.
- (2) Die Verarbeitung erfolgt ausschließlich zur Erbringung der Leistungen aus dem Hauptvertrag. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt. Der Auftragnehmer verwendet die Daten insbesondere nicht zum Training von KI-Modellen.
- (3) Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist der Auftraggeber. Er ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für die Rechtsgrundlage der Erhebung und Verarbeitung der Daten seiner Beschäftigten, allein verantwortlich.

§ 3 Weisungen

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats hierzu verpflichtet. In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
- (2) Die Weisungen sind zunächst durch den Hauptvertrag und diesen Vertrag festgelegt. Einstellungen, die der Auftraggeber in Herta selbst vornimmt, gelten als Weisung. Weitere Weisungen erteilt der Auftraggeber in Textform.
- (3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

- (4) Weisungsberechtigte Personen des Auftraggebers: [Name, Funktion, E-Mail]. Weisungen an den Auftragnehmer richtet der Auftraggeber an Datenschutz@MBD-Team.de.

§ 4 Vertraulichkeit

Der Auftragnehmer setzt bei der Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die mit den einschlägigen Datenschutzbestimmungen vertraut gemacht wurden. Die Verpflichtung gilt auch nach Beendigung ihrer Tätigkeit fort.

§ 5 Technische und organisatorische Maßnahmen

- (1) Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Vertragsschluss geltenden Maßnahmen sind in **Anlage 2** beschrieben.
- (2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie anpassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.

§ 6 Unterauftragsverarbeiter

- (1) Der Auftraggeber erteilt die allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Unterauftragsverarbeiter). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt und gelten als genehmigt.
- (2) Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen vor der Hinzuziehung oder dem Austausch 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 außerordentlich kündigen.
- (3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrages gleichwertig sind. Er haftet gegenüber dem Auftraggeber für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.
- (4) Nicht als Unterauftragsverhältnis gelten Nebenleistungen wie Telekommunikations- oder Postdienste. Der Auftragnehmer stellt auch hierfür einen angemessenen Schutz der Daten sicher.

§ 7 Unterstützung bei Rechten der betroffenen Personen

- (1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO (insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit).
- (2) Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst, sofern der Auftraggeber nichts anderes anweist.

§ 8 Unterstützung bei weiteren Pflichten des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der ihm vorliegenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei Datenschutz-Folgenabschätzungen und bei der vorherigen Konsultation der Aufsichtsbehörde. Unterstützungsleistungen, die über die Bereitstellung vorhandener Dokumentation hinausgehen und nicht durch ein Fehlverhalten des Auftragnehmers veranlasst sind, kann der Auftragnehmer nach Aufwand zu den jeweils gültigen Stundensätzen berechnen.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

- (1) Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis.
- (2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Angaben, die noch nicht vorliegen, reicht der Auftragnehmer unverzüglich nach.
- (3) Der Auftragnehmer ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und stimmt sich hierzu mit dem Auftraggeber ab.

§ 10 Nachweise und Kontrollen

- (1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung.
- (2) Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrages zu überprüfen. Der Nachweis kann vorrangig durch aktuelle Dokumentation, Selbstauskünfte, Zertifikate oder Prüfberichte erfolgen. Vor-Ort-Kontrollen sind nach rechtzeitiger Anmeldung, in der Regel mindestens zwei Wochen vorher, während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs möglich. Die Vertraulichkeit gegenüber anderen Kunden bleibt gewahrt.
- (3) Für Vor-Ort-Kontrollen kann der Auftragnehmer eine angemessene Vergütung seines Aufwands verlangen, es sei denn, die Kontrolle ergibt einen Verstoß des Auftragnehmers.

§ 11 Ort der Verarbeitung und Drittlandübermittlung

- (1) Die Verarbeitung erfolgt grundsätzlich in Rechenzentren in Deutschland.
- (2) Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Bei Nutzung des Moduls Isa können Daten an den in Anlage 3 genannten KI-Dienst übermittelt und dabei auch in den USA verarbeitet werden. Grundlage sind die Standardvertragsklauseln der EU-Kommission. Der Auftragnehmer strebt eine Verarbeitung ausschließlich in der EU an und informiert den Auftraggeber, sobald diese umgesetzt ist.
- (3) Isa wird nur aktiviert, wenn der Auftraggeber das Modul bucht. Ohne Isa findet keine Übermittlung an den KI-Dienst statt.

§ 12 Rückgabe und Löschung

- (1) Nach Ende des Hauptvertrages kann der Auftraggeber seine Daten innerhalb von 30 Tagen in einem gängigen, maschinenlesbaren Format exportieren oder deren Herausgabe verlangen.

- (2) Nach Ablauf dieser Frist löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers, einschließlich vorhandener Kopien, sofern keine gesetzliche Pflicht zur Speicherung besteht. Daten in Datensicherungen werden im Rahmen des regulären Sicherungszyklus, spätestens nach 30 Tagen, überschrieben.
- (3) Die Löschung bestätigt der Auftragnehmer auf Verlangen in Textform.

§ 13 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrages, soweit sie mit Art. 82 DSGVO vereinbar sind.

§ 14 Schlussbestimmungen

- (1) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrages vor, soweit es um den Schutz personenbezogener Daten geht.
- (2) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform.
- (3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
- (4) Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, der Sitz des Auftragnehmers.

Ort, Datum: _____

Auftraggeber: _____ Auftragnehmer: _____

Anlage 1 – Gegenstand der Verarbeitung

Modul	Zweck der Verarbeitung	Arten personenbezogener Daten	Betroffene Personen
Alle Module	Bereitstellung der Anwendung, Benutzerverwaltung, Rechte, Benachrichtigungen, Support	Name, dienstliche E-Mail, ggf. Telefon, Abteilung, Betriebsstätte, Stellenbezeichnung, Vorgesetzte, Rollen und Berechtigungen, Anmelde- und Protokolldaten	Beschäftigte des Auftraggebers, Auszubildende, freie Mitarbeitende mit Zugang
Tide – Zeiterfassung	Arbeitszeiterfassung, Pausenberechnung, Abwesenheits- und Urlaubsverwaltung, Gleitzeitkonten, Zeitrachweise, Abwesenheitslisten für die Lohnabrechnung	Kommen-/Gehen-Buchungen, Arbeitsort (Büro/Homeoffice), Pausen, Arbeitszeitmodell, Gleitzeitsalden, Abwesenheiten mit Art (z. B. Urlaub, Arbeitsunfähigkeit ohne Diagnose), Anträge und Genehmigungen, Geburtsdatum (für Pausenregeln nach JArbSchG), optional Geburtstag im Kalender, Zuschläge	wie oben

Modul	Zweck der Verarbeitung	Arten personenbezogener Daten	Betroffene Personen
Flow – Auftragsmanagement	Auftragsplanung, Zuweisung, Tätigkeitsberichte, Leistungsnachweise, Kundenverwaltung, Ablage	Zugewiesene Aufträge, Tätigkeitsberichte (Zeit, Ort, Material, Beschreibung), Dateien und Fotos, Kundendaten und Ansprechpartner (Name, Funktion, Telefon, E-Mail), Meldungen im Kundenportal	Beschäftigte des Auftraggebers; Kunden und Ansprechpartner des Auftraggebers
Isa – Wissensassistent	Beantwortung von Fragen auf Grundlage freigegebener Dokumente	Inhalte der hochgeladenen PDF-Dokumente (ggf. mit personenbezogenen Daten), gestellte Fragen und Antworten, Nutzungs- und Kostendaten	Nutzende von Isa; in Dokumenten genannte Personen

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. Abwesenheitsgründe werden nur als Art der Abwesenheit, nicht mit Diagnose erfasst. Der Auftraggeber stellt sicher, dass in Freitextfeldern und Dokumenten keine besonderen Kategorien ohne Rechtsgrundlage erfasst werden.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- Zutrittskontrolle: Betrieb der Server ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland (ISO/IEC 27001-zertifiziert) mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal. Der Auftragnehmer betreibt keine eigenen Server für Herta.
- Zugangskontrolle: personalisierte Zugänge, Passwörter mit mindestens 12 Zeichen, Zwei-Faktor-Authentisierung für Administratoren und Serverzugänge, Sperre nach mehreren fehlgeschlagenen Anmeldeversuchen.
- Zugriffskontrolle: rollenbasiertes Berechtigungskonzept in Herta (Mitarbeitende sehen nur eigene Daten; Gründe für Abwesenheiten nur für berechtigte Personen; getrennte Rechte für Abrechnen, Wissensbasis pflegen, Kosten sehen); administrative Zugriffe auf die Server nur durch die Entwickler des Auftragnehmers.
- Trennungskontrolle: logische Mandantentrennung je Organisation; getrennte Test- und Produktivsysteme.

2. Integrität

- Weitergabekontrolle: Übertragung ausschließlich verschlüsselt per TLS; Verschlüsselung der Datenträger im Ruhezustand.
- Eingabekontrolle: Protokollierung von Buchungen und Kontobewegungen als nachvollziehbare Transaktionen; Löschsperre für Aufträge mit dokumentierter Arbeit; Protokollierung administrativer Zugriffe.

3. Verfügbarkeit und Belastbarkeit

- Datensicherung: tägliche Sicherung bei der Hetzner Online GmbH in Deutschland, Aufbewahrung 30 Tage, verschlüsselt.
- Wiederherstellung: regelmäßige Tests der Wiederherstellung aus der Datensicherung.

- Schutz der Systeme: Firewall, regelmäßige Sicherheitsupdates, Überwachung der Systeme (Monitoring).

4. Verfahren zur regelmäßigen Überprüfung

- Datenschutz-Management: benannter Datenschutzbeauftragter des Auftragnehmers, erreichbar unter Datenschutz@MBD-Team.de.
- Verpflichtung der Beschäftigten auf Vertraulichkeit; regelmäßige Schulung.
- Auftragskontrolle: Unterauftragsverarbeiter nur mit AVV nach Art. 28 DSGVO.
- Überprüfung dieser Maßnahmen mindestens jährlich.

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Garantien
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Hosting der Anwendung und Datenbank	Deutschland	AVV nach Art. 28 DSGVO
OpenAI Ireland Ltd., Dublin, Irland (Konzerngesellschaft der OpenAI OpCo, LLC, USA) – nur bei gebuchtem Modul Isa	Verarbeitung von Fragen und freigegebenen Dokumenten zur Erzeugung von Antworten	EU; Verarbeitung auch in den USA möglich	Data Processing Addendum von OpenAI; Standardvertragsklauseln der EU-Kommission für Übermittlungen in die USA; keine Nutzung der Daten zum Training
Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland (Microsoft 365 / Exchange Online)	Versand von E-Mails (Zugangsdaten, Benachrichtigungen)	EU (EU-Datengrenze); Zugriffe aus den USA im Ausnahmefall möglich	Datenschutznachtrag (DPA) von Microsoft; Zertifizierung der Microsoft Corporation nach dem EU- US Data Privacy Framework; Standardvertragsklauseln
Push-Dienste der Browserhersteller (z. B. Google, Apple, Mozilla) – nur wenn Nutzende Push- Benachrichtigungen im Browser aktivieren	Zustellung von Web-Push- Benachrichtigungen	je nach Browser, auch USA	Inhalte werden nach dem Web-Push-Standard verschlüsselt übertragen; der Push-Dienst erhält nur technische Zustelldaten