

gemäß Art. 28 DSGVO**Anlage zu den Allgemeinen Geschäftsbedingungen (AGB) von BERYK Consulting GmbH**

Dieser Auftragsverarbeitungsvertrag ("AVV") ist Anlage zu den Allgemeinen Geschäftsbedingungen von BERYK Consulting GmbH und regelt die Verarbeitung personenbezogener Daten im Auftrag zwischen „Auftraggeber“ und „Auftragnehmer“.

Auftragnehmer ist:

BERYK Consulting GmbH, Friedrichstr. 155, 10117 Berlin

Stand: 14. Oktober 2026

Auftraggeber ist derjenige Nutzer, der im Rahmen der Registrierung zum Dienst quupp gemäß § 8 AGB bestätigt, als Unternehmer im Sinne von § 14 BGB zu handeln, und dabei die AGB akzeptiert. Mit dieser Registrierung und AGB-Akzeptanz wird dieser AVV automatisch und ohne gesondertes Unterschreiben Bestandteil des zwischen den Parteien bestehenden Hauptvertrags über die Nutzung des Dienstes quupp (§ 8 Abs. 3 AGB).

1 Vertragsgegenstand und Dauer

1.1 Im Rahmen des Hauptvertrags verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber Verantwortlicher im Sinne der DSGVO ist (nachfolgend „Auftraggeber-Daten“). Dieser Vertrag konkretisiert die diesbezüglichen Rechte und Pflichten der Parteien gemäß Art. 28 DSGVO.

1.2 Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrags. Er endet automatisch mit dessen Beendigung, unbeschadet der nachwirkenden Pflichten aus Ziff. 9.

2 Art und Zweck der Verarbeitung, Kategorien betroffener Personen und Datenarten

2.1 **Art und Zweck der Verarbeitung:** Automatisierte Analyse von durch den Auftraggeber hochgeladenen Dokumenten mittels KI-Sprachmodellen sowie Bereitstellung der Analyseergebnisse über die Plattform.

2.2 **Kategorien betroffener Personen:** Mitarbeiter, Kunden, Vertragspartner oder sonstige natürliche Personen, deren Daten in den vom Auftraggeber hochgeladenen Dokumenten enthalten sind.

2.3 **Kategorien personenbezogener Daten:** Stamm- und Kontaktdaten, Vertrags- und Abrechnungsdaten, Angaben zu Beschäftigung, Funktion und Qualifikation, Inhalte von Korrespondenz und Protokollen sowie alle weiteren Angaben, die in den hochgeladenen Dokumenten stehen. Hinzu kommen Name und E-Mail-Adresse der Personen, die der Auftraggeber in Projekte einlädt, und deren Kommentare und Bearbeitungen in den Projekten. Besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO dürfen nicht hochgeladen werden. Der Auftraggeber sichert zu, dass die hochgeladenen Dokumente solche Daten nicht enthalten. Die übrigen Datenarten ergeben sich aus dem jeweils hochgeladenen Dokument und werden vom Auftraggeber bestimmt.

2.4 Der Auftraggeber darf keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO in die Plattform einstellen. Eine gesonderte Einwilligung hierfür ist nicht vorgesehen.

2.5 Der Auftragnehmer darf für den eigenen Betrieb zusammengefasste Kennzahlen ohne Dokumentinhalt und ohne Personenbezug bilden, nämlich Laufzeiten, Fehlerraten und Klassifikationsstatistik. Diese Kennzahlen sind keine Auftraggeber-Daten. Eine Auswertung der hochgeladenen Dokumente oder der Analyseergebnisse für eigene Zwecke des Auftragnehmers findet nicht statt.

3 Pflichten des Auftragnehmers

3.1 Der Auftragnehmer verarbeitet Auftraggeber-Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Europäischen Union oder eines Mitgliedstaats hierzu verpflichtet; in diesem Fall unterrichtet er den Auftraggeber vor der Verarbeitung, soweit rechtlich zulässig.

3.2 Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der Auftraggeber-Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.3 Der Auftragnehmer trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO.

3.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit) sowie bei Datenschutz-Folgenabschätzungen, soweit erforderlich.

3.5 Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, mit den zur Erfüllung der Meldepflicht des Auftraggebers nach Art. 33, 34 DSGVO erforderlichen Informationen.

3.6 Bis zum Ende des Hauptvertrags und während der Frist nach § 10 Abs. 3 AGB kann der Auftraggeber seine Daten über die Exportfunktionen der Plattform herunterladen. Damit ist die Rückgabe erfüllt. Spätestens 30 Tage nach Beendigung des Hauptvertrags löscht der Auftragnehmer sämtliche Auftraggeber-Daten, sofern nicht gesetzliche Aufbewahrungspflichten entgegenstehen. Sicherungskopien werden nach 30 Tagen überschrieben.

4 Weisungsrecht des Auftraggebers

4.1 Weisungen erfolgen über die hierfür vorgesehenen Funktionen der Plattform oder in Textform. Der Auftraggeber trägt die Verantwortung für die Rechtmäßigkeit seiner Weisungen.

4.2 Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich und ist berechtigt, deren Ausführung bis zur Klärung auszusetzen.

5 Technische und organisatorische Maßnahmen

Die vom Auftragnehmer und seinen Unterauftragsverarbeitern getroffenen technischen und organisatorischen Maßnahmen sind in **Anlage 1** dargestellt.

6 Unterauftragsverarbeiter

6.1 Der Auftraggeber erteilt hiermit seine allgemeine Genehmigung zum Einsatz der in **Anlage 2** aufgeführten Unterauftragsverarbeiter.

6.2 Der Auftragnehmer informiert den Auftraggeber in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Bei Änderungen, die vom Auftragnehmer ausgehen, erfolgt die Information mindestens 10 Tage vor der Änderung. Bei Änderungen, die von einem bestehenden Unterauftragsverarbeiter ausgehen, informiert der Auftragnehmer unverzüglich nach eigener Kenntnis. Der Auftraggeber kann der Änderung aus sachlichem Grund innerhalb von 10 Tagen nach Zugang der Information widersprechen. Hält der Auftragnehmer an der Änderung fest, kann der Auftraggeber den Hauptvertrag zum Zeitpunkt der Änderung außerordentlich kündigen.

6.3 Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter zu Bedingungen, die dem in diesem AVV vereinbarten Datenschutzniveau entsprechen.

7 Kontrollrechte des Auftraggebers

7.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlichen Informationen zur Verfügung.

7.2 Der Nachweis kann vorrangig durch Vorlage aktueller Zertifizierungen (z. B. ISO 27001, C5-Testat der eingesetzten Unterauftragsverarbeiter) erfolgen, sofern hierdurch eine gleichwertige Prüfung ermöglicht wird.

7.3 Der Auftraggeber kann darüber hinaus Überprüfungen einschließlich Inspektionen vor Ort verlangen. Sie finden nach angemessener Vorankündigung während der üblichen Geschäftszeiten statt. Die Kosten einer Vor-Ort-Prüfung trägt der Auftraggeber, soweit kein Verstoß festgestellt wird.

7.4 Für Unterauftragsverarbeiter erbringt der Auftragnehmer den Nachweis vorrangig durch deren aktuelle Zertifizierungen (insbesondere ISO/IEC 27001) und Prüfberichte. Vor-Ort-Kontrollen bei Unterauftragsverarbeitern richten sich nach den Bedingungen, die diese dem Auftragnehmer einräumen.

7.5 Für Unterstützungsleistungen bei Betroffenenanfragen, Datenschutz-Folgenabschätzungen, Kontrollen und der Rückgabe von Daten kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit die

Leistung nicht durch einen Verstoß des Auftragnehmers gegen diese Vereinbarung oder geltendes Recht veranlasst ist. Der Auftragnehmer teilt die voraussichtlichen Kosten vorab mit.

8 Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Bestimmungen sowie ergänzend nach den Haftungsregelungen des Hauptvertrags (§ 9 AGB), soweit dieser AVV keine abweichenden Regelungen trifft.

9 Laufzeit, Kündigung, Schlussbestimmungen

9.1 Dieser AVV endet automatisch mit Beendigung des Hauptvertrags.

9.2 Die Pflichten aus Ziff. 3.6 (Löschung/Rückgabe) und Ziff. 3.5 (soweit zum Zeitpunkt der Beendigung noch relevant) gelten über die Vertragsbeendigung hinaus fort.

9.3 Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Dies gilt auch für einen Verzicht auf dieses Formerfordernis.

9.4 Bei Widersprüchen zwischen diesem AVV und den AGB geht dieser AVV in datenschutzrechtlichen Fragen vor.

9.5 Bei Abweichungen zwischen Sprachfassungen ist die deutsche Fassung maßgeblich.

10 Gefährdung der Daten durch Dritte

Sind die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich. Der Auftragnehmer weist alle Beteiligten darauf hin, dass die Verfügungsbefugnis über die Daten ausschließlich beim Auftraggeber als Verantwortlichem liegt.

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

Bereich	Maßnahme
Zutrittskontrolle	Die physische Zutrittskontrolle der Rechenzentren für die KI-Inferenz liegt bei IONOS Cloud GmbH und OVH SAS (OVHcloud). Die Zutrittskontrolle der Server für Anwendung, Datenbank, Objektspeicher und Mailserver liegt bei der netcup GmbH in Deutschland.
Zugangskontrolle	Anmeldung mit E-Mail und Passwort (als Hash gespeichert). Optionale Zwei-Faktor-Authentifizierung (TOTP) für Nutzer. Zugang zu den Systemen haben nur Administratoren des Auftragnehmers, und zwar nur mit Zwei-Faktor-Authentifizierung. Sie greifen nur zur Bereitstellung und zur Störungsbehebung zu.
Zugriffskontrolle	Zugriff über das eigene Konto und über Projektrollen.
Weitergabekontrolle	Transportverschlüsselung (TLS) für alle Verbindungen zur Plattform und zu den Inferenzanbietern. Die Dokumentenanalyse wird nicht in Drittländer übermittelt. Dokumentinhalte gehen nur zur Analyse an die Inferenzanbieter nach Anlage 2. Diese speichern Anfragen nicht dauerhaft und sind vertraglich verpflichtet, sie nicht zum Training von Modellen zu verwenden. Erfasst werden dort nur Metadaten wie Zeitpunkt, Modell und Tokenanzahl. Für IONOS Cloud wird auf die von IONOS Cloud ausgewiesene ISO/IEC-27001-Zertifizierung verwiesen.
Eingabekontrolle	Hochgeladene Dokumente und Aufträge werden dem Nutzerkonto zugeordnet. Anmeldungen, fehlgeschlagene Anmeldeversuche und Änderungen am Konto werden mit Zeitpunkt und IP-Adresse protokolliert.
Verfügbarkeitskontrolle	Sicherung durch Volume-Snapshots und Datenbank-Dumps (pg_dump). Sicherungen werden nach 30 Tagen bereinigt. Eine Auslagerung der Sicherungen an einen anderen Ort ist nicht zugesichert.
Trennungskontrolle	Getrennte Ablage je Nutzer. Projekte sind logisch voneinander getrennt.

Löschung	Löschung nach den Fristen der AGB und der Datenschutzerklärung. Der Auftraggeber kann Dokumente selbst löschen.
Auftragskontrolle	Vertragliche Bindung der Unterauftragsverarbeiter (Ziff. 6.3). Der Auftragnehmer aktualisiert die eingesetzte Software.
Überprüfung	Der Auftragnehmer überprüft die Maßnahmen regelmäßig, mindestens einmal im Jahr und nach wesentlichen Änderungen an den Systemen, und passt sie dem Stand der Technik an.

Anlage 2: Liste der Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Verarbeitungsort
IONOS Cloud GmbH, Elgendorfer Str. 57, 56410 Montabaur	KI-Inferenz (AI Model Hub). Wird auf Wunsch ausschließlich Deutschland vereinbart, erfolgt die Inferenz nur hier und auf den eigenen Modellen des Auftragnehmers.	Deutschland
OVH SAS (OVHcloud), 2 rue Kellermann, 59100 Roubaix	KI-Inferenz (AI Endpoints), solange nicht auf Wunsch ausschließlich Deutschland vereinbart ist	Frankreich (Gravelines)
netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe	Hosting von Anwendung, Datenbank und Objektspeicher, Mailserver für Einladungen und Benachrichtigungen	Deutschland

Die Anwendung und einen Teil der KI-Modelle betreibt der Auftragnehmer selbst. Dafür gelten die Maßnahmen nach Anlage 1. Die Haufe-Lexware GmbH & Co. KG, Munzinger Straße 9, 79111 Freiburg, erstellt mit Lexware Office die Rechnungen des Auftragnehmers. Die Mollie B.V. zieht Kreditkarte und SEPA-Lastschrift ein. Beide verarbeiten nur Rechnungs- und Zahlungsdaten des Auftraggebers, für die der Auftragnehmer selbst Verantwortlicher ist, und keine Daten aus hochgeladenen Dokumenten. Sie stehen deshalb nicht in dieser Liste und sind in der Datenschutzerklärung genannt.