Vereinbarung
über die
Auftragsverarbeitung

gemäß Art. 28 DSGVO

zwischen

dem Nutzer des Dienstes Dominion
– Verantwortlicher / Auftraggeber –

und

ORYKS | Inh. Felix Rüppel
Triftweg 17, 34125 Kassel
– Auftragsverarbeiter –

für den cloudbasierten Compliance-Dienst
Dominion (dominion.oryks.de / listenpruefung.de)

§ 1 Präambel

Diese Vereinbarung über die Auftragsverarbeitung (nachfolgend „AVV“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Nutzung des cloudbasierten Compliance-Dienstes „Dominion“ (nachfolgend „Dienst“) ergeben, der unter den Domains dominion.oryks.de und listenpruefung.de bereitgestellt wird.

Diese AVV ergänzt die Allgemeinen Geschäftsbedingungen (AGB) des Anbieters und konkretisiert die Pflichten der Vertragsparteien zum Datenschutz gemäß den Vorgaben der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DS-GVO“) sowie des Bundesdatenschutzgesetzes (BDSG).

Sie findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers im Rahmen der Diensterbringung verarbeiten.

Soweit in den AGB (dort § 9 Abs. 2) eine Auftragsverarbeitung für Sonderfälle vorgesehen ist, bildet diese AVV die hierfür erforderliche gesonderte Vereinbarung nach Art. 28 DS-GVO.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Gegenstand und Zweck

Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers personenbezogene Daten im Rahmen der Bereitstellung des Dienstes Dominion. Dominion ist eine cloudbasierte Compliance-Plattform, deren Funktionsumfang sich aus der jeweils aktuellen Leistungsbeschreibung auf der Website des Anbieters ergibt. Zum Zeitpunkt des Abschlusses dieser AVV umfasst der Dienst insbesondere folgende Funktionen:

- Sanktionslistenprüfung (Screening von Geschäftspartnern gegen internationale Sanktions- und Embargolisten)
- USt-IdNr.-Validierung (qualifizierte und einfache Bestätigung von Umsatzsteuer-Identifikationsnummern)
- KI-gestützte Ermittlung von Zolltarifnummern (automatisierte Klassifikation von Waren in den Zolltarif)

Der Auftragnehmer kann den Funktionsumfang des Dienstes um weitere Compliance-Funktionen erweitern. Sofern neue Funktionen die Art oder den Umfang der Verarbeitung personenbezogener Daten wesentlich verändern, wird Anlage 1 entsprechend aktualisiert und der Auftraggeber hierüber informiert.

Die Verarbeitung erfolgt zum Zweck der technischen Bereitstellung, Durchführung und Auswertung der jeweiligen Compliance-Prüfungen sowie der Verwaltung der Nutzerkonten.

(2) Art der verarbeiteten Daten

- Registrierungsdaten: Vorname, Nachname, E-Mail-Adresse, Unternehmen, Rolle (z. B. Key-User, User)
- Geschäftspartnerdaten: Name, Anschrift, ggf. weitere Identifikationsmerkmale (z. B. Geburtsdatum, USt-IdNr.) der vom Auftraggeber zu prüfenden Geschäftspartner – nach Wahl und Entscheidung des Auftraggebers
- Prüfergebnisse: Treffer, Klassifikationen, durchgeführte Aktionen
- Kommunikationsdaten: E-Mail-Adresse, ggf. Telefonnummer

- Technische Daten: IP-Adresse, Logdaten, Session-Informationen

(3) Kategorien betroffener Personen

- Beschäftigte und Bevollmächtigte des Auftraggebers (Nutzer des Dienstes)
- Geschäftspartner, Kunden, Lieferanten und deren Ansprechpartner, deren Daten vom Auftraggeber im Dienst verarbeitet werden

(4) Dauer

Die Laufzeit dieser AVV richtet sich nach der Laufzeit des Nutzungsvertrages (AGB § 11). Sie endet automatisch mit Beendigung des Nutzungsvertrages, sofern sich aus dieser AVV keine darüber hinausgehenden Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaates, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor Beginn der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO). Beide Parteien sind in ihren jeweiligen Rollen für die Einhaltung des geltenden Datenschutzrechts verantwortlich.

(3) Die Weisungen werden anfänglich durch den Nutzungsvertrag (AGB) und die Leistungsbeschreibung festgelegt und können vom Auftraggeber danach schriftlich oder in Textform (z. B. E-Mail) an info@oryks.de geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a) DS-GVO vor.

(2) Der Auftragnehmer wird den Auftraggeber informieren, wenn nach seiner Auffassung eine Weisung des Auftraggebers gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Der Auftragnehmer ist nicht verpflichtet, eine umfassende rechtliche Prüfung durchzuführen.

(3) Der Auftragnehmer wird technische und organisatorische Maßnahmen (TOM) zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DS-GVO genügen. Die vereinbarten TOM sind in Anlage 1 zu dieser AVV beschrieben. Der Auftragnehmer hat insbesondere Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau der

vereinbarten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anfrage mitzuteilen.

(4) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten TOM bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO (siehe hierzu ergänzend § 5).

(5) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten, insbesondere bei:

- der Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DS-GVO)
- der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DS-GVO)
- der Benachrichtigung der betroffenen Person (Art. 34 DS-GVO)
- der Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)
- der vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DS-GVO)

(6) Der Auftragnehmer unterstützt den Auftraggeber auf Anfrage bei der Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO, soweit die Auftragsverarbeitung betroffen ist.

(7) Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Der Auftragnehmer stellt ferner sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrags fortbesteht.

(8) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden, in der Art und Weise, dass der Auftraggeber seinen gesetzlichen Pflichten nach Art. 33, 34 DS-GVO nachkommen kann. Die Meldung muss mindestens folgende Angaben enthalten:

- eine Beschreibung des Vorfalls einschließlich Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze
- Kontaktdaten einer Anlaufstelle für weitere Informationen
- eine Beschreibung der voraussichtlichen Folgen und der ergriffenen oder vorgeschlagenen Abhilfemaßnahmen

Soweit die Informationen nicht gleichzeitig bereitgestellt werden können, dürfen sie ohne unangemessene Verzögerung schrittweise zur Verfügung gestellt werden.

(9) Der Auftragnehmer nennt dem Auftraggeber einen verantwortlichen Kontakt für im Rahmen dieser Vereinbarung anfallende Datenschutzfragen: info@oryks.de.

(10) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Auftragsverarbeitung beziehen.

(11) Nach Beendigung des Auftrags löscht der Auftragnehmer sämtliche personenbezogenen Daten des Auftraggebers innerhalb von 30 Tagen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Bestehen gesetzliche Aufbewahrungsfristen, erfolgt eine Sperrung der Daten bis zum Ablauf der jeweiligen Frist; anschließend werden die Daten gelöscht. Der Auftragnehmer bestätigt dem Auftraggeber die Löschung auf Anfrage. Rechnungs-

und Vertragsdaten werden gemäß den gesetzlichen Fristen (bis zu 10 Jahre) aufbewahrt. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt; hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Ergebnissen des Dienstes Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

(2) Der Auftraggeber nennt dem Auftragnehmer einen Kontakt für im Rahmen der Vereinbarung anfallende Datenschutzfragen und trägt Sorge für die Aktualität dieser Informationen.

(3) Der Auftraggeber gewährleistet, dass er zur Verarbeitung der von ihm in den Dienst hochgeladenen personenbezogenen oder unternehmerischen Daten berechtigt ist (vgl. AGB § 6 Abs. 5).

(4) Der Auftraggeber beachtet mögliche Auswirkungen bei Änderungen seiner Nutzung oder Erweiterungen auf die vorliegende AVV und teilt solche Änderungen dem Auftragnehmer unverzüglich mit. Dies kann Anpassungen in § 1 auslösen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter.

(2) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung dieser Anträge auf Weisung.

(3) Auskünfte an Dritte darf der Auftragnehmer nur erteilen, wenn er nach dem Unionsrecht oder dem Recht eines Mitgliedstaates zur Herausgabe verpflichtet ist. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtliche Anforderung vor der Auskunftserteilung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 6 Nachweismöglichkeiten und Kontrollrechte

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung alle erforderlichen Informationen zur Verfügung zu stellen. Insbesondere ist die Umsetzung der TOM gemäß Art. 32 DS-GVO nachzuweisen.

(2) Der Nachweis kann insbesondere erbracht werden durch:

- Selbstaudits
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Datenschutzbeauftragter, IT-Sicherheitsabteilung, Qualitätsauditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. ISO 27001, ISO 27701, BSI-Grundschutz)
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder Zertifizierungen gemäß Art. 42 DS-GVO

(3) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 14 Kalendertage) durchgeführt. Der Auftragnehmer darf diese von der Unterzeichnung einer Verschwiegenheitserklärung abhängig machen. Sollte der vom Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, hat der Auftragnehmer ein Einspruchsrecht. Die Anzahl der regulären Vor-Ort-Inspektionen ist auf eine Prüfung pro Kalenderjahr beschränkt. Anlassbezogene Kontrollen bleiben hiervon unberührt. Jede Partei trägt ihre eigenen Kosten.

(4) Sollte eine Datenschutzaufsichtsbehörde eine Inspektion vornehmen, gilt Absatz 3 entsprechend. Eine Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn die Aufsichtsbehörde einer gesetzlichen Verschwiegenheitspflicht unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Unterauftragsverarbeiter (Subunternehmer)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Instandhaltung von Hard- und Software oder sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz der in Anlage 2 aufgeführten Unterauftragsverarbeiter.

(3) Der Auftragnehmer informiert den Auftraggeber vor Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters schriftlich oder per E-Mail. Die Information umfasst mindestens Name, Anschrift und Kontakt des Unterauftragsverarbeiters, die unterbeauftragte Teilleistung sowie den Handlungsspielraum des Auftraggebers. Der Auftraggeber kann der Änderung innerhalb von 14 Kalendertagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung als erteilt.

(4) Erfolgt ein fristgerechter Widerspruch aus wichtigem datenschutzrechtlichem Grund, und ist eine einvernehmliche Lösungsfindung innerhalb von vier Wochen ab Eingang des Widerspruchs zwischen den Parteien nicht möglich, haben beide Parteien ein Sonderkündigungsrecht auf den von dieser Auftragsverarbeitung betroffenen Teil des Nutzungsvertrages.

(5) Für Notfallsituationen (z. B. bei dringendem Sicherheitsrisiko oder unvorhergesehenem Ausfall eines Unterauftragsverarbeiters) darf der Auftragnehmer einen Unterauftragsverarbeiter auch ohne Einhaltung der genannten Frist hinzuziehen und informiert den Auftraggeber unverzüglich.

(6) Der Auftragnehmer stellt dem Auftraggeber eine aktuelle Liste aller eingesetzten Unterauftragsverarbeiter zur Verfügung (siehe Anlage 2).

(7) Der Auftragnehmer überträgt den Unterauftragsverarbeitern gemäß Art. 28 Abs. 4 DS-GVO dieselben datenschutzrechtlichen Pflichten aus dieser Vereinbarung. Der Auftragnehmer stellt sicher, dass der Unterauftragsverarbeiter die ihm auferlegten Pflichten erfüllt. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

(8) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller hier vereinbarten Voraussetzungen für eine Unterbeauftragung gestattet.

§ 8 Übermittlung in Drittstaaten

(1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Übermittlung personenbezogener Daten in Drittstaaten außerhalb der EU bzw. des EWR findet nur statt, sofern die Voraussetzungen der Art. 44 ff. DS-GVO eingehalten werden.

(2) Soweit im Rahmen des Dienstes eine Übermittlung in die USA erfolgt (vgl. Anlage 2: OpenAI, Resend), wird das angemessene Schutzniveau durch den Abschluss von EU-Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DS-GVO sichergestellt. Zusätzlich werden technische Maßnahmen zur Datenminimierung ergriffen: Es erfolgt keine Übertragung von Kunden-IDs, internen Referenzen oder Geschäftszusammenhängen; eine dauerhafte Datenspeicherung erfolgt nicht (vgl. Datenschutzerklärung § 5 Abs. 2).

(3) Ist hierzu nichts im Vertrag vereinbart, ist die Verarbeitung in einem Drittstaat sowohl für den Auftragnehmer als auch seine Unterauftragsverarbeiter nur mit vorheriger Zustimmung des Auftraggebers zulässig.

§ 9 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

(2) Im Verhältnis der Parteien zueinander gilt die Haftungsregelung aus den AGB (§ 8 AGB) entsprechend, sofern nicht in dieser AVV ausdrücklich etwas anderes vereinbart ist.

§ 10 Kaufmännische Regelungen

(1) Es gelten die gesetzlichen und vereinbarten Mitwirkungs- und Unterstützungspflichten.

(2) Der Auftragnehmer unterstützt den Auftraggeber kostenfrei bis zu einem Kontingent von 4 Personenstunden je Kalenderjahr in folgenden Fällen:

- Unterstützung bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen gem. Kapitel III DS-GVO
- Unterstützung bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten
- Bereitstellung erforderlicher Auskünfte und Nachweis der Umsetzung der TOM
- Unterstützung bei der Durchführung von Inspektionen und Audits

(3) Bei Überschreiten des Kontingents übernimmt der Auftraggeber die durch die Unterstützungsleistungen des Auftragnehmers entstehenden Kosten zur Vergütung nach dem jeweils gültigen Stundensatz des Auftragnehmers. Dies gilt nicht, soweit der Auftragnehmer die entstandenen Aufwände schuldhaft zu vertreten hat.

§ 11 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang

Verantwortlichen darüber informieren, dass die Hoheit an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der DS-GVO liegt.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung, die auch in Textform (z. B. E-Mail) erfolgen kann, und des ausdrücklichen Hinweises, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser AVV den Regelungen der AGB vor. Sollten einzelne Teile dieser AVV unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht. Gerichtsstand ist Kassel, Deutschland.

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DS-GVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle: Hosting bei Hetzner Online GmbH und IONOS SE in deutschen Rechenzentren mit ISO 27001-Zertifizierung, physischer Zutrittskontrolle und Überwachung.

Zugangskontrolle: Passwort-Hashing, 2-Faktor-Authentifizierung für Admin-Zugänge, Least-Privilege-Zugriffskonzepte, automatische Session-Timeouts.

Zugriffskontrolle: Rollenbasierte Berechtigungen (Key-User / User), Firewalls, Zugriffsprotokollierung.

Trennungskontrolle: Mandantentrennung auf Datenbankebene, logische Trennung der Kundendaten.

Pseudonymisierung und Verschlüsselung: TLS-Verschlüsselung für Datenübertragung, Datenminimierung bei KI-Anfragen an Drittanbieter (keine Übertragung von Kunden-IDs oder Geschäftszusammenhängen).

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle: Verschlüsselte Übertragung (TLS), Protokollierung von Datenübermittlungen.

Eingabekontrolle: Nachvollziehbarkeit von Dateneingaben, -änderungen und -löschungen durch Logdaten und Prüfprotokolle.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DS-GVO)

Verfügbarkeitskontrolle: Kontinuierliche Backups, Nutzung redundanter Rechenzentrums-Infrastruktur, geplante Wartungsarbeiten mit Vorankündigung (AGB § 7).

Belastbarkeit: Skalierbare Cloud-Infrastruktur, Überwachung der Systemlast.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DS-GVO)

Regelmäßige Sicherheitsaudits, Schwachstellenscans, Überprüfung und Aktualisierung der TOM bei Bedarf, CSRF-Schutz, reguläre Softwareupdates und Patch-Management.

Anlage 2: Übersicht der Unterauftragsverarbeiter

Unterauftrags-verarbeiter	Beschreibung der Teilleistung	Ort der Daten-verarbeitung	Transfermechanismus
Hetzner Online GmbH, Gunzenhausen, DE	Server-Hosting, Infrastruktur für Anwendung und selbst gehostete KI-Modelle	Deutschland	Nicht erforderlich (EU)
IONOS SE, Montabaur, DE	Server-Hosting, E-Mail-Infrastruktur (IONOS-Postfach)	Deutschland	Nicht erforderlich (EU)
MongoDB, Inc., 1633 Broadway, 38th Floor, New York, NY 10019, USA	Datenbankhosting (Verschluesselung ruhender Daten mit AES-256; keine Nutzung der Daten zu eigenen Zwecken	Deutschland	EU-Standardvertragsklauseln (SCCs) nach Art. 46 Abs. 2 lit. c DS-GVO
OpenAI, LLC, San Francisco, USA	KI-basierte Funktionen (z. B. Klassifikation); keine Übertragung von Kunden-IDs, internen Referenzen oder Geschäftszusammenhängen; keine dauerhafte Speicherung; keine Nutzung zu Trainingszwecken	USA	EU-Standardvertrags-klauseln (SCCs) nach Art. 46 Abs. 2 lit. c DS-GVO
Resend, Inc., San Francisco, USA	Transaktionaler E-Mail-Versand (z. B. Nutzereinladungen, Passwort-Reset) unter Verwendung eines IONOS-Postfaches	USA (Versand-infrastruktur); Deutschland (Postfach)	EU-Standardvertrags-klauseln (SCCs) nach Art. 46 Abs. 2 lit. c DS-GVO

Unterschriften

Diese Vereinbarung tritt mit Abschluss des Nutzungsvertrages (Registrierung und Bestellung gemäß AGB § 2) in Kraft und bedarf keiner gesonderten Unterschrift, sofern die Parteien nicht ausdrücklich eine schriftliche Unterzeichnung vereinbaren.

Optional: Bei Bedarf können die Parteien diese AVV zusätzlich handschriftlich oder qualifiziert elektronisch unterzeichnen:

Für den Auftraggeber:	**Für den Auftragnehmer:** ORYKS | Inh. Felix Rüppel
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift