CORGENT

by Malango Tech

Auftragsverarbeitungsvertrag

Art. 28 DSGVO · Data Processing Agreement (DPA)

Dieser Auftragsverarbeitungsvertrag regelt die Verarbeitung personenbezogener Daten durch die Malango Tech UG
(haftungsbeschränkt) i.G., handelnd unter der Marke „Corgent“, wenn sie als Auftragsverarbeiter im Auftrag des
Kunden im Zusammenhang mit der Corgent-KI-Agentenplattform und den damit verbundenen Diensten tätig wird. Er
beinhaltet die EU-Standardvertragsklauseln und behandelt Übermittlungen in das Vereinigte Königreich und in die Schweiz.

Dokument	Auftragsverarbeitungsvertrag (AVV / DPA)
Version	1.0
Gültig ab	24. Juni 2026
Auftragsverarbeiter	Malango Tech UG (haftungsbeschränkt) i.G. — „Corgent“
Eingetragene Anschrift	Schumannstraße 24, 71640 Ludwigsburg, Deutschland
Datenschutzkontakt	mk@corgent.ai
Anwendbares Recht	Bundesrepublik Deutschland

Inhalt

Hintergrund

Dieser Auftragsverarbeitungsvertrag einschließlich seiner Anhänge (der **„AVV“** oder **„DPA“**) ist Bestandteil des zwischen dem Kunden und Corgent geschlossenen Vertrags über die Bereitstellung der Dienste (der **„Hauptvertrag“**) und wird in diesen einbezogen. Er dokumentiert die Vereinbarung der Parteien hinsichtlich der Verarbeitung von Kundenpersonenbezogenen Daten und wird gemäß Art. 28 Abs. 3 der Verordnung (EU) 2016/679 (die **„DSGVO“**) sowie weiterer anwendbarer Datenschutzgesetze geschlossen.

Soweit der Kunde als Verantwortlicher handelt und Corgent als Auftragsverarbeiter in Bezug auf Kundenpersonenbezogene Daten tätig wird, findet dieser AVV Anwendung. Soweit der Kunde selbst als Auftragsverarbeiter im Auftrag eines Drittverantwortlichen handelt, tritt Corgent als Unterauftragsverarbeiter auf und dieser AVV findet *mutatis mutandis* Anwendung. Im Falle eines Widerspruchs zwischen diesem AVV und dem Hauptvertrag in Bezug auf den Gegenstand des Datenschutzes hat dieser AVV Vorrang; im Falle eines Widerspruchs zwischen diesem AVV und den Standardvertragsklauseln haben die Standardvertragsklauseln Vorrang.

Die Parteien

Auftragsverarbeiter: Malango Tech UG (haftungsbeschränkt) i.G., handelnd unter der Marke „Corgent“, Schumannstraße 24, 71640 Ludwigsburg, Deutschland, vertreten durch den Geschäftsführer Maximilian Koch („ **Corgent** “, der „ **Auftragsverarbeiter** “).

Kunde: Die juristische Person oder natürliche Person, die den Hauptvertrag mit Corgent geschlossen hat und in Bezug auf Kundenpersonenbezogene Daten als Verantwortlicher (oder Auftragsverarbeiter) handelt (der „ **Kunde** “, der „ **Verantwortliche** “).

Gemeinsam: Der Kunde und Corgent sind jeweils eine „ **Partei** “ und gemeinsam die „ **Parteien** “.

Unternehmensstatus: Gesellschaft in Gründung (i.G.). Die Eintragung in das Handelsregister ist beim Amtsgericht Stuttgart beantragt; die Handelsregisternummer wird nach Eintragung ergänzt. Die Umsatzsteuer-Identifikationsnummer wurde beim Bundeszentralamt für Steuern beantragt und wird nach Erteilung ergänzt. Bis zur Eintragung haften die handelnden Personen persönlich.

1. Definitionen und Auslegung

1.1 Großgeschriebene Begriffe, die in diesem AVV verwendet, aber nicht definiert sind, haben die im Hauptvertrag festgelegte Bedeutung. Für diesen AVV gelten folgende Definitionen:

- **„Anwendbare Datenschutzgesetze“** bezeichnet alle Gesetze und Vorschriften, die auf die Verarbeitung personenbezogener Daten im Rahmen dieses AVV anwendbar sind, einschließlich der DSGVO; des Bundesdatenschutzgesetzes (BDSG); der UK GDPR und des UK Data Protection Act 2018 (die **„UK-Datenschutzgesetze“**); des Schweizer Bundesgesetzes über den Datenschutz (das **„Schweizer DSG“**); und, soweit anwendbar, US-amerikanischer bundesstaatlicher Datenschutzgesetze.
- **„Verantwortlicher“** , **„Auftragsverarbeiter“** , **„betroffene Person“** , **„personenbezogene Daten“** , **„Verarbeitung“** , **„Verletzung des Schutzes personenbezogener Daten“** und **„Aufsichtsbehörde“** haben die in Art. 4 DSGVO festgelegten Bedeutungen (oder die gleichwertigen Begriffe, wie „business“ und „service provider“, nach anderen anwendbaren Datenschutzgesetzen).
- **„Kundenpersonenbezogene Daten“** bezeichnet alle personenbezogenen Daten, die Corgent im Auftrag des Kunden im Rahmen der Bereitstellung der Dienste verarbeitet, wie in Anhang I näher beschrieben.
- **„Dienste“** bezeichnet die Corgent-KI-Agentenplattform und die damit verbundenen Produkte, die im Rahmen des Hauptvertrags bereitgestellt werden, einschließlich der Entdeckung, Bereitstellung, Konfiguration und Ausführung von KI-Agenten, der Manager-Chat-Erfahrung, vom Kunden aktivierter Integrationen und der zugehörigen APIs.

- **„Standardvertragsklauseln“** oder **„SCCs“** bezeichnet die von der Europäischen Kommission in der Durchführungsentscheidung (EU) 2021/914 vom 4. Juni 2021 angenommenen Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, wie in Anhang IV näher spezifiziert.
- **„UK Addendum“** bezeichnet den International Data Transfer Addendum zu den EU-Standardvertragsklauseln, der vom UK Information Commissioner gemäß § 119A des UK Data Protection Act 2018 herausgegeben wurde, Version B1.0.
- **„Unterauftragsverarbeiter“** bezeichnet jeden Auftragsverarbeiter (einschließlich verbundener Unternehmen von Corgent oder Dritter), den Corgent mit der Verarbeitung von Kundenpersonenbezogenen Daten beauftragt, wie in Anhang III aufgeführt.
- **„US-amerikanische bundesstaatliche Datenschutzgesetze“** bezeichnet die jeweils geltenden US-amerikanischen bundesstaatlichen Datenschutzgesetze, einschließlich des California Consumer Privacy Act in der jeweils geltenden Fassung (der **„CCPA“**).

1.2 Überschriften dienen lediglich der Übersichtlichkeit und beeinflussen die Auslegung nicht. Verweise auf ein Gesetz oder eine gesetzliche Bestimmung umfassen nachgeordnete Rechtsvorschriften sowie jede Änderung, Neufassung oder Ersetzung desselben. Die Wörter „einschließlich“, „insbesondere“ und „unter anderem“ sind ohne Einschränkung zu verstehen.

2. Geltungsbereich, Rollen der Parteien und Rangfolge

2.1 Dieser AVV findet Anwendung, soweit und in dem Umfang, in dem Corgent Kundenpersonenbezogene Daten im Auftrag des Kunden im Rahmen der Bereitstellung der Dienste verarbeitet. Er ergänzt und ersetzt nicht andere datenschutzrechtliche Pflichten der Parteien aus dem Hauptvertrag oder anwendbaren Datenschutzgesetzen.

2.2 In Bezug auf Kundenpersonenbezogene Daten ist der Kunde der Verantwortliche (oder, soweit der Kunde selbst Auftragsverarbeiter für einen Drittverantwortlichen ist, ein Auftragsverarbeiter) und Corgent ist der Auftragsverarbeiter (oder Unterauftragsverarbeiter). Jede Partei ist für die Einhaltung der ihr nach anwendbaren Datenschutzgesetzen obliegenden Pflichten verantwortlich.

2.3 Corgent handelt darüber hinaus als **eigenständiger Verantwortlicher** in Bezug auf bestimmte begrenzte Daten, die es für eigene Geschäftszwecke verarbeitet (wie Kontoverwaltung, Abrechnung, Sicherheit, Betrugsprävention und Verbesserung der Dienste). Eine solche Verarbeitung ist in Abschnitt 16 beschrieben und unterliegt der Corgent-Datenschutzerklärung und nicht den Verantwortlicher-zu-Auftragsverarbeiter-Bestimmungen dieses AVV.

2.4 Rangfolge. Im Falle eines Widerspruchs oder einer Unstimmigkeit gilt folgende Rangfolge, wobei das höher eingestufte Dokument im Falle eines Widerspruchs in Bezug auf den Gegenstand des Datenschutzes Vorrang hat: (i) die Standardvertragsklauseln (und jedes UK- oder Schweizer Übermittlungsmechanismus); (ii) dieser AVV einschließlich seiner Anhänge; (iii) der Hauptvertrag.

3. Gegenstand und Einzelheiten der Verarbeitung

3.1 Gegenstand, Art und Zweck der Verarbeitung, die Arten der Kundenpersonenbezogenen Daten, die Kategorien betroffener Personen und die Dauer der Verarbeitung sind in **Anhang I (Beschreibung der Verarbeitung)** beschrieben, der integraler Bestandteil dieses AVV ist.

3.2 Corgent verarbeitet Kundenpersonenbezogene Daten nur zu den in Anhang I beschriebenen Zwecken und nur gemäß den dokumentierten Weisungen des Kunden, einschließlich in Bezug auf Übermittlungen von Kundenpersonenbezogenen Daten in ein Drittland, es sei denn, Corgent ist nach Unionsrecht oder dem Recht eines Mitgliedstaats, dem es unterliegt, zur Verarbeitung

solcher Daten verpflichtet. In einem solchen Fall informiert Corgent den Kunden vor der Verarbeitung über diese gesetzliche Verpflichtung, es sei denn, dieses Recht verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses.

3.3 Die Weisungen des Kunden ergeben sich aus diesem AVV und dem Hauptvertrag und können durch die Konfigurationsentscheidungen des Kunden innerhalb der Dienste ergänzt werden (zum Beispiel die vom Kunden aktivierten Agenten und Integrationen, die vom Kunden übermittelten Eingaben, Aufbewahrungseinstellungen und Genehmigungsmodi im Manager-Chat). Zusätzliche oder geänderte Weisungen müssen schriftlich (einschließlich Textform) vereinbart werden und können einer Anpassung der Gebühren unterliegen, soweit sie einen wesentlichen Mehraufwand erfordern.

3.4 Corgent informiert den Kunden unverzüglich, wenn es der Auffassung ist, dass eine Weisung gegen anwendbare Datenschutzgesetze verstößt. Corgent kann die Ausführung der betreffenden Weisung aussetzen, bis sie vom Kunden bestätigt oder geändert wird, ohne dass dies einen Verstoß gegen den Hauptvertrag darstellt.

4. Pflichten von Corgent als Auftragsverarbeiter

Corgent verpflichtet sich:

- Kundenpersonenbezogene Daten nur auf dokumentierte Weisungen des Kunden zu verarbeiten, wie in Abschnitt 3 festgelegt, einschließlich in Bezug auf internationale Übermittlungen;
- sicherzustellen, dass Personen, die zur Verarbeitung von Kundenpersonenbezogenen Daten befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Vertraulichkeitspflicht unterliegen, und geeigneten Zugangskontrollen und Schulungen unterworfen sind;
- die in **Anhang II** festgelegten technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO umzusetzen und aufrechtzuerhalten;
- die in Abschnitt 6 festgelegten Bedingungen für die Beauftragung von Unterauftragsverarbeitern einzuhalten;
- unter Berücksichtigung der Art der Verarbeitung den Kunden durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung der Pflicht des Kunden zu unterstützen, auf Anfragen betroffener Personen zur Ausübung ihrer Rechte zu reagieren (Abschnitt 7);
- den Kunden bei der Gewährleistung der Einhaltung der Pflichten nach den Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzungen und vorherige Konsultation) zu unterstützen, unter Berücksichtigung der Art der Verarbeitung und der Corgent zur Verfügung stehenden Informationen;
- nach Wahl des Kunden nach Beendigung der Bereitstellung der Dienste alle Kundenpersonenbezogenen Daten zu löschen oder zurückzugeben und vorhandene Kopien zu löschen, es sei denn, die Aufbewahrung ist gesetzlich vorgeschrieben (Abschnitt 12); und
- dem Kunden alle zur Nachweisung der Einhaltung der in Art. 28 DSGVO festgelegten Pflichten erforderlichen Informationen zur Verfügung zu stellen und Prüfungen, einschließlich Inspektionen, wie in Abschnitt 11 festgelegt, zu ermöglichen und daran mitzuwirken.

4.1 Corgent verarbeitet Kundenpersonenbezogene Daten nicht für eigene Zwecke außerhalb des Rahmens der Weisungen des Kunden und verkauft oder „teilt“ Kundenpersonenbezogene Daten nicht (wie diese Begriffe in US-amerikanischen bundesstaatlichen Datenschutzgesetzen definiert sind), noch behält, nutzt oder offenbart es Kundenpersonenbezogene Daten außerhalb der unmittelbaren Geschäftsbeziehung oder zu anderen Zwecken als der Erbringung der Dienste.

4.2 Corgent führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten, die im Auftrag des Kunden durchgeführt werden, gemäß Art. 30 Abs. 2 DSGVO und stellt dieses Verzeichnis dem Kunden oder einer zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung.

5. Pflichten und Weisungen des Kunden

5.1 Der Kunde ist dafür verantwortlich sicherzustellen, dass er über eine gültige Rechtsgrundlage nach anwendbaren Datenschutzgesetzen für die Verarbeitung von Kundenpersonenbezogenen Daten und für die Übermittlung solcher Daten an Corgent verfügt und dass er alle erforderlichen Hinweise erteilt und alle erforderlichen Einwilligungen von betroffenen Personen eingeholt hat.

5.2 Der Kunde gewährleistet, dass seine Weisungen, einschließlich der Konfiguration von Agenten, Integrationen und an die Dienste übermittelten Eingaben, den anwendbaren Datenschutzgesetzen entsprechen und dass er die Dienste nicht zur Verarbeitung personenbezogener Daten in einer Weise nutzen wird, die die in Anhang I beschriebenen Zwecke überschreitet oder mit ihnen unvereinbar ist.

5.3 Datenminimierung. Die Dienste sind universell einsetzbare KI-Werkzeuge. Der Kunde ist dafür verantwortlich zu bestimmen, welche Daten er übermittelt. Der Kunde darf keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO), Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) oder andere besonders sensible Daten in Prompts, Anhängen oder Agenteneingaben übermitteln, es sei denn, dies ist unbedingt erforderlich, rechtmäßig und mit angemessenen Schutzmaßnahmen vereinbar. Der Kunde wird ermutigt, unnötige Identifikatoren aus Prompts zu entfernen und nur die für die jeweilige Aufgabe erforderlichen Daten zu übermitteln.

5.4 Genehmigungsmodi. Soweit die Dienste manuelle und automatische Genehmigungsmodi für von KI-Agenten oder dem Manager-Chat durchgeführte Aktionen anbieten, ist der Kunde dafür verantwortlich, den Modus und die Berechtigungen entsprechend seinem Risikoprofil auszuwählen, und bleibt für die Überwachung, Validierung und Rückgängigmachung automatisierter Aktionen verantwortlich.

5.5 Soweit der Kunde als Auftragsverarbeiter im Auftrag eines Drittverantwortlichen handelt, stellt er sicher, dass er von diesem Verantwortlichen ermächtigt ist, Corgent als Unterauftragsverarbeiter zu den Bedingungen dieses AVV zu bestellen.

6. Unterauftragsverarbeiter

6.1 Der Kunde erteilt die **allgemeine schriftliche Genehmigung** für Corgent, Unterauftragsverarbeiter mit der Verarbeitung von Kundenpersonenbezogenen Daten zu beauftragen, vorbehaltlich dieses Abschnitts 6. Die von Corgent zum Gültigkeitsdatum beauftragten Unterauftragsverarbeiter sind in **Anhang III** zusammen mit ihrer Rolle, ihrem Standort, ihrem Übermittlungsprofil und ihrem Löschpfad aufgeführt. Eine aktuelle Liste wird unter corgent.ai/subprocessors veröffentlicht (die **„Unterauftragsverarbeiterliste“**).

6.2 Corgent verpflichtet jeden Unterauftragsverarbeiter durch einen schriftlichen Vertrag zu datenschutzrechtlichen Pflichten, die nicht weniger schützend sind als die in diesem AVV festgelegten, und gewährt insbesondere ausreichende Garantien für die Umsetzung angemessener technischer und organisatorischer Maßnahmen gemäß Art. 28 Abs. 4 DSGVO. Corgent haftet dem Kunden gegenüber uneingeschränkt für die Erfüllung der Pflichten jedes Unterauftragsverarbeiters.

6.3 Mitteilung von Änderungen. Corgent teilt dem Kunden mindestens **dreißig (30) Tage** im Voraus die Hinzufügung oder Ersetzung eines Unterauftragsverarbeiters mit, indem es die Unterauftragsverarbeiterliste aktualisiert und/oder den Kunden über die Dienste oder per E-Mail

benachrichtigt, und gibt dem Kunden damit die Möglichkeit, aus angemessenen datenschutzrechtlichen Gründen zu widersprechen, bevor der neue Unterauftragsverarbeiter mit der Verarbeitung von Kundenpersonenbezogenen Daten beginnt.

6.4 Widerspruch. Widerspricht der Kunde innerhalb von fünfzehn (15) Tagen nach der Mitteilung schriftlich aus angemessenen datenschutzrechtlichen Gründen, arbeiten die Parteien in gutem Glauben zusammen, um eine für beide Seiten akzeptable Lösung zu finden. Wird keine Lösung erzielt, kann der Kunde als einziges und ausschließliches Rechtsmittel den betroffenen Teil der Dienste gemäß dem Hauptvertrag kündigen.

6.5 Vom Kunden aktivierte Integrationen (zum Beispiel Google oder Microsoft) werden nur beauftragt, wenn der Kunde sie verbindet und einen Teil des Datenflusses an den jeweiligen Anbieter weiterleitet, der im Auftrag des Kunden handelt; die Beziehung des Kunden zu solchen Anbietern kann zusätzlich durch die eigenen Vereinbarungen des Kunden mit diesen geregelt sein.

7. Unterstützung bei Rechten betroffener Personen

7.1 Corgent benachrichtigt den Kunden unverzüglich, wenn es (oder ein Unterauftragsverarbeiter) eine Anfrage einer betroffenen Person zur Ausübung von Rechten auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch oder des Rechts, nicht einer ausschließlich automatisierten Entscheidung unterworfen zu werden (eine **„Anfrage einer betroffenen Person“**) in Bezug auf Kundenpersonenbezogene Daten erhält, und antwortet nicht selbst auf eine solche Anfrage, es sei denn auf dokumentierte Weisung des Kunden oder soweit gesetzlich vorgeschrieben.

7.2 Unter Berücksichtigung der Art der Verarbeitung leistet Corgent angemessene Unterstützung, einschließlich durch geeignete technische und organisatorische Maßnahmen und über Self-Service-Funktionalität, soweit verfügbar, um dem Kunden zu ermöglichen, innerhalb der von anwendbaren Datenschutzgesetzen gesetzten Fristen auf Anfragen betroffener Personen zu reagieren.

7.3 Corgent betreibt einen Workflow für Anfragen betroffener Personen (DSAR), der die primäre Löschung in von Corgent kontrollierten Systemen koordiniert und, soweit anwendbar, Folgeanfragen an relevante Unterauftragsverarbeiter stellt. Einige Unterauftragsverarbeiter erfordern separate Löschanfragen nach der primären Löschung, wie in Anhang III angegeben.

8. Meldung von Verletzungen des Schutzes personenbezogener Daten

8.1 Corgent benachrichtigt den Kunden unverzüglich und, soweit möglich, spätestens innerhalb von **zweiundsiebzig (72) Stunden** , nachdem es von einer Verletzung des Schutzes personenbezogener Daten, die Kundenpersonenbezogene Daten betrifft, Kenntnis erlangt hat, um dem Kunden zu ermöglichen, seinen eigenen Meldepflichten nach den Art. 33 und 34 DSGVO nachzukommen.

8.2 Die Benachrichtigung beschreibt, soweit bekannt und sobald Informationen verfügbar werden, die Art der Verletzung des Schutzes personenbezogener Daten (einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl betroffener Personen und betroffener Datensätze); die wahrscheinlichen Folgen; die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Minderung ihrer Auswirkungen; sowie den Namen und die Kontaktdaten einer zuständigen Ansprechperson. Ist es nicht möglich, alle Informationen auf einmal bereitzustellen, kann Corgent diese in Phasen ohne weitere unangemessene Verzögerung bereitstellen.

8.3 Corgent ergreift angemessene Schritte zur Eindämmung, Untersuchung und Minderung jeder Verletzung des Schutzes personenbezogener Daten und arbeitet angemessen mit dem Kunden

bei dessen Untersuchung, Meldung und Abhilfe zusammen. Die Benachrichtigung oder Reaktion von Corgent auf eine Verletzung des Schutzes personenbezogener Daten gilt nicht als Anerkennung eines Verschuldens oder einer Haftung durch Corgent.

9. Sicherheit der Verarbeitung (Art. 32 DSGVO)

9.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung und der Risiken für die Rechte und Freiheiten natürlicher Personen setzt Corgent angemessene technische und organisatorische Maßnahmen um und unterhält diese, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, wie in **Anhang II** beschrieben.

9.2 Corgent kann die Maßnahmen in Anhang II von Zeit zu Zeit aktualisieren oder ändern, sofern solche Aktualisierungen das Gesamtsicherheitsniveau der Dienste während der Laufzeit des Hauptvertrags nicht wesentlich verringern.

9.3 Corgent stellt sicher, dass der Zugang zu Kundenpersonenbezogenen Daten auf Personal beschränkt ist, das einen solchen Zugang zur Erfüllung des Hauptvertrags benötigt, und wendet rollenbasierte Zugangskontrollen, das Prinzip der geringsten Rechte und Mandantenisolation (einschließlich Row-Level Security auf Datenbankebene) an, wie in Anhang II näher beschrieben.

10. Internationale Datenübermittlungen

10.1 Corgent hostet Kundenpersonenbezogene Daten vorrangig innerhalb der Europäischen Union (Supabase, Region Frankfurt, eu-central-1). Corgent übermittelt Kundenpersonenbezogene Daten nicht in ein Land außerhalb des Europäischen Wirtschaftsraums (**„EWR“**), des Vereinigten Königreichs oder der Schweiz, es sei denn, ein angemessener Übermittlungsmechanismus nach anwendbaren Datenschutzgesetzen ist vorhanden.

10.2 Soweit eine Übermittlung von Kundenpersonenbezogenen Daten aus dem EWR in ein Drittland erfolgt, für das kein Angemessenheitsbeschluss vorliegt (zum Beispiel an einen in den USA ansässigen Monitoring-Unterauftragsverarbeiter oder an Modellanbieter hinter OpenRouter außerhalb der EU), finden die **Standardvertragsklauseln** Anwendung und werden durch Verweis in diesen AVV einbezogen, wie in **Anhang IV** ausgefüllt. Für Übermittlungen, die UK-Datenschutzgesetzen unterliegen, findet das **UK Addendum** Anwendung; für Übermittlungen, die dem Schweizer DSG unterliegen, finden die SCCs mit den in Anhang IV festgelegten Änderungen Anwendung. Modellinferenz über OpenRouter läuft mit Zero-Data-Retention (ZDR) und data_collection=deny; je nach gewähltem Modell kann die Inferenz auf Anbieter-Infrastruktur außerhalb der EU stattfinden, abgesichert durch die Standardvertragsklauseln gemäß dieser Ziffer.

10.3 Mit dem Abschluss dieses AVV gelten die Parteien als die Standardvertragsklauseln (und, soweit anwendbar, das UK Addendum) wie in Anhang IV dargestellt ab dem Gültigkeitsdatum unterzeichnet. Im Falle eines Widerspruchs zwischen den Standardvertragsklauseln und diesem AVV haben die Standardvertragsklauseln Vorrang.

10.4 Corgent setzt ergänzende Maßnahmen ein, soweit erforderlich (wie Verschlüsselung bei der Übertragung und im Ruhezustand, Datenminimierung und vertragliche Verpflichtungen zur Einschränkung behördlicher Zugriffsanfragen), und stellt auf Anfrage Informationen zur Verfügung, die zum Nachweis erforderlich sind, dass Übermittlungen gemäß anwendbaren Datenschutzgesetzen durchgeführt werden. Für Modellinferenz über OpenRouter setzt Corgent als Standardkonfiguration Zero-Data-Retention (ZDR) sowie data_collection=deny ein; Drittlandübermittlungen im Rahmen der Inferenz sind durch die Standardvertragsklauseln abgesichert.

11. Prüfungen, Informationen und Compliance

11.1 Corgent stellt dem Kunden alle zur Nachweisung der Einhaltung von Art. 28 DSGVO und dieses AVV erforderlichen Informationen zur Verfügung und ermöglicht Prüfungen, einschließlich Inspektionen, die vom Kunden oder einem vom Kunden beauftragten Prüfer durchgeführt werden, und wirkt daran mit.

11.2 Um Störungen zu minimieren und die Vertraulichkeit und Sicherheit anderer Kunden zu schützen, werden die Prüfungsrechte des Kunden zunächst dadurch erfüllt, dass Corgent relevante Dokumentation, Sicherheitszusammenfassungen und etwaige Zertifizierungen oder Prüfberichte Dritter (wie die seiner Hosting- und Infrastruktur-Unterauftragsverarbeiter) zur Verfügung stellt. Der Kunde kann solche Unterlagen höchstens einmal pro Kalenderjahr anfordern, es sei denn, dies ist von einer Aufsichtsbehörde vorgeschrieben oder folgt auf eine Verletzung des Schutzes personenbezogener Daten.

11.3 Soweit die nach Ziffer 11.2 bereitgestellte Dokumentation nicht ausreicht, um die Einhaltung nachzuweisen, kann der Kunde nach angemessener vorheriger schriftlicher Mitteilung von mindestens dreißig (30) Tagen während der üblichen Geschäftszeiten eine Vor-Ort- oder Fernprüfung durchführen, vorbehaltlich angemessener Vertraulichkeits- und Sicherheitsanforderungen und höchstens einmal pro Kalenderjahr. Jede Partei trägt ihre eigenen Kosten, wobei der Kunde die angemessenen Kosten von Corgent für Unterstützung über ein *de-minimis* -Niveau hinaus erstattet. Die Ergebnisse jeder Prüfung sind vertrauliche Informationen beider Parteien.

11.4 Corgent benachrichtigt den Kunden unverzüglich, wenn es feststellt, dass es seinen Pflichten aus diesem AVV nicht mehr nachkommen kann, woraufhin der Kunde die Übermittlung von Kundenpersonenbezogenen Daten aussetzen und/oder die betroffenen Dienste kündigen kann.

12. Rückgabe und Löschung von Kundenpersonenbezogenen Daten

12.1 Bei Beendigung oder Ablauf des Hauptvertrags oder jederzeit auf schriftliche Anfrage des Kunden löscht oder gibt Corgent nach Wahl des Kunden alle Kundenpersonenbezogenen Daten zurück und löscht vorhandene Kopien, es sei denn, Unionsrecht oder das Recht eines Mitgliedstaats erfordert eine fortgesetzte Aufbewahrung.

12.2 Corgent schließt eine solche Löschung innerhalb eines angemessenen Zeitraums ab, der die in Anhang III beschriebenen Aufbewahrungsfristen nicht überschreitet, unter Berücksichtigung von Backup-Zyklen. In flüchtigen Caches und Job-Warteschlangen gespeicherte Kundenpersonenbezogene Daten unterliegen der Time-to-Live-Ablaufzeit (TTL), typischerweise innerhalb von vierundzwanzig (24) Stunden. Für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zur Einhaltung gesetzlicher Aufbewahrungspflichten (zum Beispiel Finanz- und Steuerunterlagen) aufbewahrte Daten werden nur so lange und nur in dem Umfang aufbewahrt, wie erforderlich, und unterliegen weiterhin den Schutzmaßnahmen dieses AVV.

12.3 Auf Anfrage bestätigt Corgent schriftlich (einschließlich Textform), dass es diesen Abschnitt 12 eingehalten hat.

13. Haftung und Freistellung

13.1 Die Haftung jeder Partei aus oder im Zusammenhang mit diesem AVV, ob vertraglich, deliktisch oder anderweitig, unterliegt den im Hauptvertrag festgelegten Haftungsbeschränkungen und -ausschlüssen. Jeder Verweis im Hauptvertrag auf die Haftung einer Partei bezeichnet die Gesamthaftung dieser Partei aus dem Hauptvertrag und diesem

AVV zusammen.

13.2 Nichts in diesem AVV beschränkt oder schließt eine Haftung aus, die nach anwendbaren Datenschutzgesetzen nicht beschränkt oder ausgeschlossen werden kann, einschließlich der Haftung der Parteien gegenüber betroffenen Personen nach Art. 82 DSGVO oder der Haftungsbestimmungen der Standardvertragsklauseln. Im Verhältnis der Parteien zueinander wird die Haftung entsprechend der jeweiligen Verantwortung jeder Partei für den durch die Verarbeitung verursachten Schaden zugewiesen.

14. Laufzeit, Änderung und Fortgeltung

14.1 Dieser AVV tritt am Gültigkeitsdatum in Kraft und bleibt in Kraft, solange Corgent Kundenpersonenbezogene Daten im Auftrag des Kunden verarbeitet. Bestimmungen, die ihrer Natur nach die Beendigung überdauern sollen (einschließlich solcher zu Vertraulichkeit, Löschung, Übermittlungen, Haftung und anwendbarem Recht), gelten über die Beendigung dieses AVV und des Hauptvertrags hinaus fort.

14.2 Die Parteien verhandeln in gutem Glauben über Änderungen dieses AVV, die erforderlich sind, um Änderungen anwendbarer Datenschutzgesetze, Leitlinien von Aufsichtsbehörden oder die Ungültigkeit oder Ersetzung eines Übermittlungsmechanismus zu berücksichtigen. Corgent kann diesen AVV nach angemessener Mitteilung aktualisieren, soweit dies zur Aufrechterhaltung der Compliance erforderlich ist, sofern eine solche Aktualisierung die Rechte des Kunden nicht wesentlich beeinträchtigt.

15. Allgemeine Bestimmungen

15.1 Anwendbares Recht und Gerichtsstand. Dieser AVV unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG) und der Kollisionsnormen, unbeschadet zwingenden Verbraucherschutzrechts und der Rechtswahl- und Gerichtsstandsbestimmungen der Standardvertragsklauseln. Die Gerichte am eingetragenen Sitz von Corgent sind ausschließlich zuständig, soweit gesetzlich zulässig.

15.2 Mitteilungen. Datenschutzmitteilungen an Corgent sind an mk@corgent.ai zu richten. Mitteilungen an den Kunden sind an die mit dem Kundenkonto verknüpften Kontaktdaten oder wie anderweitig im Hauptvertrag festgelegt zu richten.

15.3 Salvatorische Klausel. Sollte eine Bestimmung dieses AVV unwirksam oder undurchsetzbar sein oder werden, bleiben die übrigen Bestimmungen in vollem Umfang wirksam, und die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame Bestimmung, die ihrer wirtschaftlichen und rechtlichen Absicht am nächsten kommt.

15.4 Gesamtvereinbarung. Dieser AVV bildet zusammen mit seinen Anhängen und den Standardvertragsklauseln die gesamte Vereinbarung der Parteien in Bezug auf die Verarbeitung von Kundenpersonenbezogenen Daten und ersetzt alle früheren Auftragsverarbeitungsbedingungen zum gleichen Gegenstand.

15.5 Elektronische Ausführung. Die Parteien vereinbaren, dass die Annahme des Hauptvertrags oder die Nutzung der Dienste nach dem Gültigkeitsdatum dieselbe Wirkung hat wie die Unterzeichnung dieses AVV und der darin einbezogenen Standardvertragsklauseln.

16. Corgent als eigenständiger Verantwortlicher (Konto- und Betriebsdaten)

16.1 Die Parteien erkennen an, dass Corgent in Bezug auf bestimmte begrenzte Daten als eigenständiger Verantwortlicher und nicht als Auftragsverarbeiter handelt. Dies umfasst Daten zur Kontoregistrierung und -verwaltung, Abrechnungs- und Guthabendaten, Authentifizierungsidentifikatoren, Sicherheits-, Missbrauchspräventions- und Audit-Protokolle

sowie aggregierte oder anonymisierte Nutzungsstatistiken zur Betreibung, Absicherung und Verbesserung der Dienste (**„Konto- und Betriebsdaten“**).

16.2 Corgent verarbeitet Konto- und Betriebsdaten gemäß anwendbaren Datenschutzgesetzen und seiner Datenschutzerklärung auf Rechtsgrundlagen einschließlich der Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) und seiner berechtigten Interessen am sicheren, zuverlässigen und rechtmäßigen Betrieb der Dienste (Art. 6 Abs. 1 lit. f DSGVO). Soweit erforderlich, holt Corgent eine Einwilligung ein (Art. 6 Abs. 1 lit. a DSGVO), zum Beispiel für nicht wesentliche Analysen.

16.3 Anonymisierte Daten. Erstellt Corgent aggregierte oder anonymisierte Daten, unterhält und nutzt es solche Daten nur in anonymisierter Form und versucht nicht, sie wieder zu identifizieren, es sei denn, dies ist nach anwendbaren Datenschutzgesetzen zulässig.

Vereinbart durch die Parteien

Mit der Annahme des Hauptvertrags oder durch die fortgesetzte Nutzung der Dienste erklärt sich jede Partei ab dem Gültigkeitsdatum an diesen AVV gebunden. Soweit eine handschriftliche Unterzeichnung erforderlich ist, können die Parteien den AVV unten unterzeichnen.

Für Corgent (Auftragsverarbeiter)	**Für den Kunden (Verantwortlicher)**
Unterschrift: _____	Unterschrift: _____
Name: _____	Name: _____
Funktion: _____	Funktion: _____
Unternehmen: Malango Tech UG (haftungsbeschränkt) i.G.	Unternehmen: _____
Datum: _____	Datum: _____

Anhang I

Beschreibung der Verarbeitung (SCC-Anhang I)

A. Liste der Parteien

Datenexporteur / Verantwortlicher: Der Kunde, wie im Hauptvertrag und in seinem Kontodatensatz identifiziert. Rolle: Verantwortlicher (oder Auftragsverarbeiter im Auftrag eines Drittverantwortlichen).

Datenimporteur / Auftragsverarbeiter: Malango Tech UG (haftungsbeschränkt) i.G., handelnd unter der Marke „Corgent“, Schumannstraße 24, 71640 Ludwigsburg, Deutschland. Kontakt: Maximilian Koch, mk@corgent.ai. Rolle: Auftragsverarbeiter.

Für die Übermittlung relevante Tätigkeiten: Bereitstellung der Corgent-KI-Agentenplattform und der zugehörigen Dienste für den Datenexporteur.

B. Beschreibung der Übermittlung

Kategorien betroffener Personen: Die autorisierten Nutzer des Kunden; die eigenen Endkunden und Kontakte des Kunden, deren Daten der Kunde übermittelt; Absender und Empfänger von Inhalten, die von Agenten verarbeitet werden (zum Beispiel E-Mail- oder Supportkontakte); und alle anderen natürlichen Personen, deren personenbezogene Daten in von dem Kunden übermittelten Eingaben enthalten sind.

Kategorien personenbezogener Daten: Konto- und Kontaktidentifikatoren (Name, E-Mail, Rolle); Authentifizierungsidentifikatoren; vom Kunden übermittelte Prompts, Anhänge und Agenteneingaben sowie darin enthaltene personenbezogene Daten; von Agenten generierte Ausgaben; Integrationsinhalte (zum Beispiel, soweit verbunden, E-Mail- oder Kalenderdaten); Nutzungs-, Abrechnungs- und Transaktionsmetadaten; sowie technische/Protokolldaten wie IP-Adresse und Anfragemetadaten.

Besondere Datenkategorien: Nicht vorgesehen. Die Dienste sind nicht für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) oder Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) ausgelegt. Solche Daten dürfen nicht übermittelt werden, es sei denn, dies ist unbedingt erforderlich, rechtmäßig und mit vom Kunden festgelegten angemessenen Schutzmaßnahmen vereinbar (siehe Ziffer 5.3).

Häufigkeit der Übermittlung: Fortlaufend, für die Dauer der Bereitstellung der Dienste.

Art der Verarbeitung: Hosting, Speicherung, Übertragung, Routing an Modellanbieter zur Inferenz, Ausführung von Agentenlogik und Integrationen, Caching und Warteschlangen, Analysen (soweit aktiviert), Fehlerüberwachung, Abrechnungsberechnung und Löschung.

Zweck der Verarbeitung: Bereitstellung, Aufrechterhaltung, Absicherung und Unterstützung der Dienste gemäß den Weisungen des Kunden und dem Hauptvertrag.

Dauer der Verarbeitung: Für die Laufzeit des Hauptvertrags und bis zur Löschung oder Rückgabe gemäß Abschnitt 12, vorbehaltlich gesetzlicher Aufbewahrungspflichten.

Unterauftragsverarbeiter: Wie in Anhang III festgelegt. Der Zeitraum, für den Unterauftragsverarbeiter Daten verarbeiten, entspricht der oben genannten Dauer.

C. Zuständige Aufsichtsbehörde

Die zuständige Aufsichtsbehörde ist die federführende Behörde für den Datenexporteur (soweit der Datenexporteur im EWR niedergelassen ist) oder andernfalls die Aufsichtsbehörde des EWR-Mitgliedstaats, in dem der EU-Vertreter des Datenexporteurs niedergelassen ist. Soweit Corgent als Exporteur handelt, ist die zuständige Behörde der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

Anhang II

Technische und organisatorische Maßnahmen (SCC-Anhang II · Art. 32 DSGVO)

Corgent unterhält die folgenden technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Diese Maßnahmen können sich weiterentwickeln, sofern das Gesamtschutzniveau nicht wesentlich verringert wird.

1. Pseudonymisierung und Verschlüsselung

- Verschlüsselung personenbezogener Daten bei der Übertragung mittels TLS (HTTPS/WSS) für alle externen Verbindungen.
- Verschlüsselung personenbezogener Daten im Ruhezustand für die primäre Datenbank, den Objektspeicher und die vom Hosting-Unterauftragsverarbeiter bereitgestellten Backups.
- Geheimnisse, API-Schlüssel und OAuth-Token werden mittels Verschlüsselung und zugangskontrolliertem Secret Management gespeichert; Integrations-Token sind verschlüsselt und widerrufbar.
- Minimierung und, soweit möglich, Pseudonymisierung von Identifikatoren in Analysen und Protokollen; sensible Nutzdaten sind in der Produktion von Analysen ausgeschlossen.

2. Vertraulichkeit (Zugangskontrolle)

- Rollenbasierte Zugangskontrolle und das Prinzip der geringsten Rechte für Personal und Dienste.
- Mandantenisolation auf Anwendungs- und Datenbankebene, einschließlich PostgreSQL Row-Level Security (RLS).
- Authentifizierung über einen verwalteten Identity Provider mit JWT-basierten Sitzungen; administrativer Zugang ist auf eine definierte Gruppe autorisierter Nutzeridentifikatoren beschränkt.
- Personal ist an Vertraulichkeitspflichten gebunden und erhält angemessene Sicherheits- und Datenschutzschulungen.

3. Integrität

- Audit-Protokollierung sicherheitsrelevanter und administrativer Ereignisse, einschließlich Einwilligungsänderungen und Workflows für Anfragen betroffener Personen.
- Eingabevalidierung und Schema-Validierung (einschließlich für Agenten-Manifeste und API-Anfragen) zur Reduzierung von Injektions- und Missbrauchsrisiken.
- Content Security Policy, Transportschutz und Ratenbegrenzung zur Abwehr von Missbrauch und zum Schutz der Verfügbarkeit.

4. Verfügbarkeit und Belastbarkeit

- Nutzung verwalteter, redundanter Cloud-Infrastruktur mit automatisierten Backups für den primären Datenspeicher.
- Hintergrund-Worker und Job-Warteschlangen mit kontrollierten Wiederholungen; flüchtige Cache- und Warteschlangendaten sind TTL-gebunden (typischerweise ≤ 24 Stunden).
- Monitoring und Fehlerverfolgung zur Erkennung, Analyse und Behebung betrieblicher Probleme.

5. Wiederherstellung und Tests

- Fähigkeit, Verfügbarkeit und Zugang zu personenbezogenen Daten nach einem Vorfall zeitnah aus Backups wiederherzustellen.

- Regelmäßige Überprüfung der Sicherheitskonfiguration und Abhängigkeitshygiene im Rahmen des Entwicklungszyklus.

6. Governance, Unterauftragsverarbeitung und Incident Response

- Ein dokumentierter Prozess zur Beauftragung und Bewertung von Unterauftragsverarbeitern mit vertraglicher Weitergabe datenschutzrechtlicher Pflichten.
- Ein Prozess zur Reaktion auf Verletzungen des Schutzes personenbezogener Daten, der darauf ausgelegt ist, den Kunden unverzüglich zu benachrichtigen (Ziffer 8.1).
- Ein DSAR-Prozess zur Koordination der primären Löschung und der Nachverfolgung bei Unterauftragsverarbeitern.
- Es werden keine undokumentierten „Hintertüren“ in die Dienste eingebaut, um Dritten Zugang zu personenbezogenen Daten zu verschaffen.

Anhang III

Liste der Unterauftragsverarbeiter

Die folgenden Unterauftragsverarbeiter sind zum Gültigkeitsdatum zur Verarbeitung von Kundenpersonenbezogenen Daten autorisiert. Die aktuelle Liste einschließlich etwaiger Aktualisierungen wird unter corgent.ai/subprocessors veröffentlicht. Als „vom Kunden aktiviert“ gekennzeichnete Integrations-Unterauftragsverarbeiter verarbeiten Daten nur, wenn der Kunde die jeweilige Integration verbindet.

Unterauftragsverarbeiter	Zweck & Datenkategorien	Region & Übermittlungsprofil	Aufbewahrung / Löschung
Supabase	Kern-Datenbank, Authentifizierung und Objektspeicher-Hosting. Kontodaten, Anwendungsdatensätze, Auth-Identifikatoren, hochgeladene Dateien.	Europäische Union (Frankfurt, eu-central-1). Primäre Datenbank und Speicher in der EU gehostet.	Primärer Löschpfad über Corgent-Kontolöschung und den DSAR-Workflow.
OpenRouter	Modell-Routing und Inferenzausführung. Prompts, Anhang-Metadaten, Modellnutzungsmetadaten.	OpenRouter (USA) mit Modellanbietern in der EU und in Drittländern; Inferenzstandort abhängig vom gewählten Modell. Zero-Data-Retention (ZDR) und data_collection=deny als Standard; AVV/DPA mit Standardvertragsklauseln vorhanden.	Anbieter-Support-Workflow und vertraglicher AVV-Kanal.
Stripe	Guthabenkauf und Auszahlungsabwicklung. Abrechnungsidentifikatoren, Zahlungsmethoden-Metadaten, Transaktionsmetadaten.	EU-Entität (Stripe Payments Europe, Ltd.) mit Standardvertragskontrollen für Weiterübermittlungen.	Aufbewahrung aufseiten des Auftragsverarbeiters gebunden an gesetzliche Finanzpflichten.
Resend	Transaktions-E-Mail-Zustellung. Empfänger-E-Mail, Nachrichtenmetadaten, Zustellprotokolle.	EU-Region für die konfigurierte Versanddomäne (eu-west-1) mit Anbieterschutzmaßnahmen.	Anbieter-Supportanfrage und Aufbewahrungsrichtlinien-Kontrollen.
PostHog	Produktanalysen (nur bei erteilter Analyse-Einwilligung). Pseudonyme Identifikatoren, Seitenaufrufe, Feature-Nutzungsmetadaten.	EU Cloud (eu.i.posthog.com). In der EU gehostet; LLM-Nutzdaten in der Produktion ausgeschlossen.	Personenlöschung über PostHog-API und Widerruf der Einwilligung.
Sentry	Anwendungsfehlerüberwachung (nur bei erteilter Performance-Einwilligung). Fehlertelemetrie; Stack Traces mit entfernten personenbezogenen Daten.	Vereinigte Staaten. Drittlands-Auftragsverarbeiter unter SCCs; personenbezogene Daten vor Übermittlung entfernt.	Löschanfrage auf Issue-Ebene und Aufbewahrungskontrollen.
Railway	API- und Hintergrund-Worker-Hosting. Anfragemetadaten, flüchtige Warteschlangen-Nutzdaten.	Europa (Produktionsregion). Infrastruktur-Auftragsverarbeiter; vorübergehende Verarbeitung von API-Verkehr.	Protokollaufbewahrungslimits und Infrastrukturvertragskanal.
Netlify	Statische Frontend-Bereitstellung und Edge Functions. HTTP-Zugriffsprotokolle, CDN-Anfragemetadaten.	Globales CDN-Edge-Netzwerk. Edge-Delivery-Auftragsverarbeiter unter SCCs; keine primäre Datenspeicherung.	Protokollaufbewahrung gemäß Netlify-Richtlinie.

Unterauftragsverarbeiter	Zweck & Datenkategorien	Region & Übermittlungsprofil	Aufbewahrung / Löschung
Redis (via Railway)	Flüchtiger Cache, Job-Warteschlangen und Ratenbegrenzungsstatus. Sitzungs-Cache-Schlüssel, TTL-gebundene Warteschlangen-Job-Nutzdaten.	Co-lokalisiert mit der Railway-Anwendungsregion. Vorübergehende Verarbeitung; TTL ≤ 24h.	Automatischer TTL-Ablauf und Schlüssellöschung bei Kontolöschung.
Google (Gmail / Cloud) — *vom Kunden aktiviert*	Gmail- und Google-Cloud-Integrationen, wenn vom Kunden verbunden. E-Mail-Inhalte, OAuth-Token, Integrationsmetadaten.	Global (Region des Google-Kontos des Kunden). Nur aktiviert, wenn der Kunde die Integration verbindet.	Token-Widerruf, Google-Kontokontrollen und Corgent-Löschung.
Microsoft Graph — *vom Kunden aktiviert*	Microsoft-365-Integrationen, wenn vom Kunden verbunden. E-Mail-/Kalendermetadaten, OAuth-Token.	Global (Region des Microsoft-Mandanten des Kunden). Nur aktiviert, wenn der Kunde die Integration verbindet.	Token-Widerruf, Microsoft-Kontokontrollen und Corgent-Löschung.

Datenschutzbedingungen der Unterauftragsverarbeiter

- Supabase — supabase.com/legal/dpa
- OpenRouter — openrouter.ai/privacy
- Stripe — stripe.com/legal/dpa
- Resend — resend.com/legal/dpa
- PostHog — posthog.com/dpa
- Sentry — sentry.io/legal/dpa/
- Railway — railway.com/legal/dpa
- Netlify — netlify.com/legal/dpa/
- Google — cloud.google.com/terms/data-processing-addendum
- Microsoft — microsoft.com/licensing (Products and Services Data Protection Addendum)

Anhang IV

Standardvertragsklauseln — Auswahl und grenzüberschreitende Bestimmungen

1. EU-Standardvertragsklauseln

Soweit die SCCs gemäß Abschnitt 10 Anwendung finden, werden die SCCs (Durchführungsentscheidung (EU) 2021/914) durch Verweis in diesen AVV einbezogen und wie folgt ausgefüllt:

- **Module.** Modul Zwei (Verantwortlicher zu Auftragsverarbeiter) findet Anwendung, soweit der Kunde Verantwortlicher ist. Modul Drei (Auftragsverarbeiter zu Auftragsverarbeiter) findet Anwendung, soweit der Kunde als Auftragsverarbeiter im Auftrag eines Drittverantwortlichen handelt.
- **Klausel 7 (Andockklausel).** Findet Anwendung.
- **Klausel 9 (Einsatz von Unterauftragsverarbeitern).** Option 2 (allgemeine schriftliche Genehmigung) findet Anwendung. Die Mindestmitteilungsfrist für Änderungen bei Unterauftragsverarbeitern beträgt dreißig (30) Tage, wie in Ziffer 6.3 dieses AVV festgelegt.
- **Klausel 11 (Rechtsbehelfe).** Der optionale unabhängige Streitbeilegungsmechanismus findet keine Anwendung.
- **Klausel 17 (Anwendbares Recht).** Die SCCs unterliegen dem Recht der Bundesrepublik Deutschland.
- **Klausel 18 (Gerichtsstand und Zuständigkeit).** Streitigkeiten werden vor den Gerichten Deutschlands beigelegt.
- **Anhang I, II und III zu den SCCs.** Werden durch Anhang I, Anhang II und Anhang III dieses AVV ausgefüllt.

2. UK Addendum

Für Übermittlungen, die UK-Datenschutzgesetzen unterliegen, wird das UK Addendum (Version B1.0) einbezogen und findet auf die SCCs Anwendung. Tabelle 1 (Parteien) wird durch Anhang I.A ausgefüllt; Tabellen 2 und 3 werden durch Verweis auf die EU-SCCs und die oben genannten Anhänge ausgefüllt; und in Tabelle 4 darf keine Partei das Addendum beenden, wie in Abschnitt 19 dargestellt, es sei denn, dies ist durch das Addendum zulässig. Das „Startdatum“ ist das Gültigkeitsdatum.

3. Schweizer DSG

Für Übermittlungen, die dem Schweizer DSG unterliegen, finden die SCCs mit folgenden Änderungen Anwendung: (i) Verweise auf die DSGVO sind als Verweise auf das Schweizer DSG zu verstehen, soweit die Übermittlung diesem unterliegt; (ii) die zuständige Aufsichtsbehörde ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB); (iii) der Begriff „Mitgliedstaat“ darf nicht so ausgelegt werden, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte am gewöhnlichen Aufenthaltsort geltend zu machen; und (iv) die SCCs schützen auch die Daten juristischer Personen bis zum Inkrafttreten gleichwertiger Revisionen, soweit dies nach dem Schweizer DSG erforderlich ist.

4. Übermittlungen aus anderen Rechtsordnungen

Soweit personenbezogene Daten einer Übermittlung unterliegen, die den Datenschutzgesetzen einer anderen Rechtsordnung unterliegt und einen gleichwertigen Übermittlungsmechanismus erfordert, finden die SCCs mit den Änderungen Anwendung, die erforderlich sind, um den von den Gesetzen dieser Rechtsordnung geforderten gleichwertigen Schutz zu gewährleisten, und die Rollen des

jeweiligen Datenexporteurs und -importeurs werden entsprechend ausgelegt.

Ende des Auftragsverarbeitungsvertrags. Dieses Dokument wird von Corgent programmatisch zur Transparenz und Vertragsvereinfachung erzeugt. Es handelt sich um eine Vorlage und stellt keine Rechtsberatung dar; der Kunde sollte für seine spezifischen Umstände eigene Beratung einholen.