VERTRAG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG EINES VERANTWORTLICHEN („*AVV*“)

STAND 21.02.2026

zwischen

Cambioo FlexCo

Siolygasse 20B/6, 1190 Wien

Österreich

- nachfolgend „*die Auftragsverarbeiterin*“ genannt -

und

dem Kunden gemäß § 1 der AGB der Cambioo FlexCo
(abrufbar unter https://www.cambioo.ai/agb)

- nachfolgend „*die Verantwortliche*“ genannt -

- Verantwortliche und Auftragsverarbeiterin gemeinsam „*die Parteien*“ genannt -

werden ergänzend zu den AGB über das „KI-Telefon“ der Verantwortlichen folgende

Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 DSGVO vereinbart:

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die

Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 15 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass

der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere

Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r): der Kunde gemäß § 1 der AGB der Cambioo FlexCo

Auftragsverarbeiter: Cambioo FlexCo

Adresse: Siolygasse 20B/6, 1190 Wien, Österreich
Telefon: +43 699 13816505
Email: office@cambioo.ai

https://www.cambioo.ai

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden und Kategorien personenbezogener Daten, die verarbeitet werden

Kategorien der Personen, die von der Verarbeitung betroffen sein können	**Datenarten**
Endkunden	Telefonnummer
	Weitere Informationen, die während des Anrufs mitgeteilt werden:
	Name
	E-Mail-Adresse
	Adresse (Straße, Hausnummer, Türnummer, PLZ, Stadt, Land)
	Details zum Anliegen des Endkunden
	Datum und Uhrzeit des Termins
	Nachricht des Endkunden
	Bei Geschäftskunden zusätzlich: Unternehmensspezifische Informationen
Mitarbeiter:innen von Endkunden	Telefonnummer
	Weitere Informationen, die während des Anrufs mitgeteilt werden:
	Name
	E-Mail-Adresse
	Funktion
Interessenten	Datenarten wie bei Endkunden oben
Mitarbeiter:innen von Interessenten	Datenarten wie bei Mitarbeiter:innen von Endkunden oben
Verantwortlicher	Unternehmensspezifische Informationen (Informationen zu Objekten/Immobilien, Websites, Kontaktdaten, Factsheets, …)
Mitarbeiter:innen von Verantwortlichem	Name

	Telefonnummer
	E-Mail-Adresse
	Funktion

Besondere Kategorien personenbezogener Daten werden nicht gezielt erhoben und sind für die Erfüllung des Auftrags nicht erforderlich. Es kann jedoch nicht ausgeschlossen werden, dass die betroffenen Personen in ihrer Nachricht freiwillig besondere Kategorien personenbezogener Daten bekannt geben. Die erhobenen Daten werden nicht nach diesen Kriterien durchsucht oder ausgewertet.

Art der Verarbeitung

Umfasst sind sämtliche Verarbeitungstätigkeiten des Auftragsverarbeiters zur Erfüllung der vertraglichen Pflichten gemäß Pilot-SaaS-Vertrag sowie eines gegebenenfalls darauf folgenden Vertrags über die Nutzung des KI-Telefons.

Der Auftragsverarbeiter bietet eine Software as a Service (SaaS)-Lösung in Form einer KI-gestützten Telefonassistenz-Dienstleistung an („Software“). Die Software soll mit Künstlicher Intelligenz den Inbound-Telefonassistenzbereich des Kunden verbessern, dabei kann sie die Funktion eines digitalen Front Desk übernehmen und als erste Anlaufstelle des Kunden in Form einer KI-basierten Rezeption direkt oder als KI-Anrufbeantwortung (also wenn ein Mensch nicht abheben sollte) Anrufe entgegennehmen oder beantworten. Bei speziellen Anliegen des Anrufers leitet die Software den Anruf gezielt an das zuständige Fachpersonal des Kunden weiter und/oder nimmt das Anliegen auf.

Es handelt es sich insbesondere um folgende Funktionalitäten:

1) Knowledgebase & FAQs: Die Software verfügt über ein umfassendes Wissen über die vom Verantwortlichen zur Verfügung gestellten Informationen. Sie kann daher sowohl allgemeine als auch spezifische Fragen des Anrufers beantworten.
2) Weiterleitung von Anrufen: Bei komplexen Anfragen kann die Software den Anruf an das zuständige Fachpersonal weiterleiten.
3) Terminvereinbarung: Die Software ist in der Lage, Termine zu vereinbaren (Google Calendar, Outlook, …) .
4) Verknüpfung zu anderen Systemen: Die Software kann Informationen aus anderen Softwaresystemen (CRM Systeme, …) über die API-Schnittstelle auslesen und auch neue Informationen einspeisen.
5) Verarbeitung des Transkripts: Das Transkript wird gespeichert und verarbeitet. Die Software erstellt eine Zusammenfassung und kann daraus Schlüsseldaten wie Name und Adresse extrahieren. Auch die Dauer des Telefonats und die Telefonnummer werden gespeichert. Diese Daten werden zur Fehleranalyse gespeichert und können dem Verantwortlichen bei Bedarf per E-Mail oder in einem Dashboard zur Verfügung gestellt werden. Dadurch bekommt der Verantwortliche einen Überblick über die Anrufe und es kann bei gewissen Anliegen eine weitere Bearbeitung durch Mitarbeiter stattfinden.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

1) Beantwortung von Kundenanfragen, Kundenberatung
2) Pflege von Kundenbeziehungen
3) Kundenkommunikation und -hilfe
4) Beschwerdemanagement
5) Aufzeichnung von Kundenanrufen zu Qualitätssicherungszwecken

Dauer der Verarbeitung

Entspricht der Laufzeit des Pilot-SaaS-Vertrags sowie gegebenenfalls der Laufzeit eines darauf folgenden Vertrags über die Nutzung des KI-Telefons. Sofern ein solcher Anschlussvertrag abgeschlossen wird, verlängert sich die Laufzeit automatisch entsprechend den vertraglich vereinbarten Bedingungen dieses Anschlussvertrags.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Siehe Anlage IV

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Vorbemerkung: Daten des Verantwortlichen werden ganz überwiegend oder fast ausschließlich im System des Unterauftragsverarbeiters Nr. 1 gemäß Anhang IV gespeichert. Der Auftragsverarbeiter selbst bzw. seine Mitarbeiter greifen lediglich durch Endgeräte auf die Systeme des Unterauftragsverarbeiters Nr. 1 zu. Es kommt daher maßgeblich auf die technischen und organisatorischen Maßnahmen beim Unterauftragsverarbeiter Nr. 1 an, die in der AVV (https://www.ovh.de/support/agb/Auftragsverarbeitungsvertrag.pdf) beschrieben sind.

Entsprechend können maßgebliche Daten über die Systeme der weiteren Unterauftragsverarbeiter gemäß Anhang IV laufen, sodass es maßgeblich auch auf die dortigen technischen Maßnahmen ankommt. Die technischen und organisatorischen Maßnahmen des jeweiligen Unterauftragsverarbeiters Anhang IV sind in der Übersicht im Anhang IV verlinkt.

Technische und organisatorische Maßnahmen beim Auftragsverarbeiter selbst sind damit vorrangig mit Blick auf einen sicheren und vertraulichen Zugang auf die Systeme der Unterauftragsverarbeiter gemäß Anhang IV zu ergreifen.

Auf der Grundlage dieses Sachverhalts werden die folgenden technischen und organisatorischen Maßnahmen getroffen:

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung:

- Zugangsbeschränkungen: Nur Personen, die direkt an der Verarbeitung beteiligt sind, haben Zugang zu den Systemen und Daten.
- Regelmäßige Passwortänderungen: Passwörter werden regelmäßig geändert, um die Sicherheit zu erhöhen.
- Eingeschränkte Sichtbarkeit und Änderungsrechte: Nur autorisiertes Personal kann die Daten sehen und ändern.
- Implementierung von Benutzername/Passwort-Authentifizierung mit gültigen Passwortregelungen: Jeder Benutzer muss sich mit einem eindeutigen Benutzernamen und einem sicheren Passwort authentifizieren.
- Verwendung von Rollen und Berechtigungen nach dem “Need-to-know-Grundsatz”: Zugriff auf Daten und Systeme wird nur Personen gewährt, die diesen für ihre Aufgaben benötigen.
- Grundlegende Sicherheitsvorkehrungen zum Schutz der Server vor Angriffen und unbefugtem Zugriff sind implementiert: Maßnahmen wie Firewalls und Anti-Malware-Software sind in Verwendung.
- Ausfallsicherheit der Systeme: Unsere Systeme sind so gestaltet, dass sie auch bei technischen Problemen weiterarbeiten und die Datenverfügbarkeit gewährleistet ist.
- Alarmsystem: Ein Alarmsystem benachrichtigt das Team sofort bei großen Fehlern, Incidents oder Errors.

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:

- Sicherungs- und Wiederherstellungskonzept: der Serveranbieter OVHcloud bietet automatische Backups der Daten an.

- Externe Datensicherung: Eine Sicherung in einem anderen physischen Datencenter wird als Zusatzleistung angeboten.
- Redundanz und Ausfallsicherheit: Unsere Systeme sind ausfallsicher gestaltet, um sicherzustellen, dass Daten auch bei technischen Problemen verfügbar bleiben. Eine komplette Ausfallsicherheit gibt es nicht, jedoch wird eine höhere Redundanz als Zusatzleistung angeboten.
- Alarmsystem: Ein Alarmsystem benachrichtigt das Team sofort bei großen Fehlern, Incidents oder Errors, sodass sofortige Maßnahmen zur Wiederherstellung der Daten ergriffen werden können.
- Kontinuierliche Überwachung: Unsere Systeme werden kontinuierlich überwacht, um sicherzustellen, dass sie stets ordnungsgemäß funktionieren und im Notfall schnell wiederhergestellt werden können.
- Dokumentierte Notfallpläne: Notfallpläne sind dokumentiert, um sicherzustellen, dass im Falle eines Zwischenfalls alle notwendigen Schritte zur Wiederherstellung der Daten schnell und effizient durchgeführt werden können.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung:

- Regelmäßige Überprüfung: Die Serverintegrität wird regelmäßig überprüft, es wird nach möglichen Schwachstellen gesucht und sichergestellt, dass alle Systeme ordnungsgemäß funktionieren und ausfallsicher sind.
- Bewertung und Evaluierung: Die technischen und organisatorischen Maßnahmen werden regelmäßig bewertet und ihre Wirksamkeit überprüft. Dies umfasst die Analyse der aktuellen Sicherheitsprotokolle und die Anpassung an neue Bedrohungen und Technologien.
- Protokollierung und Dokumentation: Alle Überprüfungen und Bewertungen werden protokolliert und dokumentiert, um eine nachvollziehbare Historie der Sicherheitsmaßnahmen zu führen und kontinuierliche Verbesserungen zu ermöglichen.
- Aktualisierung der Maßnahmen: Basierend auf den Ergebnissen der Überprüfungen und Bewertungen werden die technischen und organisatorischen Maßnahmen kontinuierlich aktualisiert und verbessert, um den aktuellen Sicherheitsanforderungen gerecht zu werden.
- Schulung: Mitarbeiter:innen, die mit personenbezogenen Daten arbeiten, werden laufend für den sorgfältigen Umgang mit Daten sensibilisiert.

Maßnahmen zur Identifizierung und Autorisierung der Nutzer:

- Benutzername/Passwort-Authentifizierung
- Rollenbasierte Zugriffskontrolle

Maßnahmen zum Schutz der Daten während der Übermittlung:

- Verschlüsselung der Datenübertragung: TLS (Transport Layer Security) ist implementiert, um die Daten während der Übermittlung zu schützen.

Maßnahmen zum Schutz der Daten während der Speicherung:

- Verschlüsselung: Die Laptops der Mitarbeiter:innen des Auftragsverarbeiters sind verschlüsselt und entsprechend gesichert.
- Zugriffskontrollen: Strikte Zugriffskontrollen, die sicherstellen, dass nur autorisierte Personen Zugriff auf die gespeicherten Daten haben, sind implementiert. Dies schließt die Verwendung von starken Authentifizierungsmechanismen und rollenbasierten Zugriffskontrollen ein.

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

- Externe Datenverarbeitung: Die Daten werden extern bei OVHcloud gehostet, wodurch die physische Sicherheit von deren Rechenzentren gewährleistet wird.
- Keine eigenen Serverräume: Da wir keine eigenen Serverräume betreiben, sind keine speziellen physischen Sicherheitsmaßnahmen vor Ort erforderlich.

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

- Grundlegende Protokollierungsfunktionen: Es werden grundlegende Protokollierungsfunktionen genutzt, die erfassen, wer wann welche Daten eingegeben, geändert oder gelöscht hat.
- Zugriffsprotokolle: Protokollierung aller Zugriffe auf Systeme und Daten, um nachvollziehen zu können, wer wann auf welche Informationen zugegriffen hat.
- Überwachung und Analyse: Regelmäßige Überprüfung und Analyse der Protokolldaten, um ungewöhnliche Aktivitäten oder Sicherheitsvorfälle frühzeitig zu erkennen.

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

- Standardkonfigurationen: Alle Systeme und Anwendungen werden mit sicheren Standardkonfigurationen eingerichtet, um eine einheitliche und sichere Basis zu gewährleisten.
- Wir entfernen unnötige Dienste-, Anwender- und Benutzerkonten
- Regelmäßige Überprüfungen: Systemkonfigurationen werden regelmäßig überprüft und auditiert, um sicherzustellen, dass sie den aktuellen Sicherheitsanforderungen entsprechen.
- Ansible wird als Konfigurationsmanagement Tool genutzt.

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

- IT-Sicherheitsrichtlinien: Implementierung und regelmäßige Aktualisierung von IT-Sicherheitsrichtlinien, die klare Vorgaben und Verhaltensregeln für alle Mitarbeiter festlegen.
- Verantwortlichkeiten: Klare Zuweisung von Verantwortlichkeiten für die IT und IT-Sicherheit innerhalb des Unternehmens. Jede Rolle ist genau definiert, und die entsprechenden Personen sind für die Einhaltung der Sicherheitsmaßnahmen verantwortlich.

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

- Prozessdokumentation: Detaillierte Dokumentation aller Prozesse, um Transparenz und Nachvollziehbarkeit zu gewährleisten und die Grundlage für kontinuierliche Verbesserungen zu schaffen.

- Kundenzufriedenheitsanalysen: Regelmäßige Analysen der Kundenzufriedenheit, um Feedback zu Prozessen und Produkten zu erhalten und Verbesserungen vorzunehmen.

Maßnahmen zur Gewährleistung der Datenminimierung

- Wir achten darauf nur notwendige Daten zu speichern und vermeiden die Erhebung von Daten "auf Vorrat". Gespeicherte Daten sind an einen Zweck gebunden und werden nicht zweckentfremdet.
- Daten werden momentan nicht automatisch gelöscht, dies kann jedoch bei Bedarf implementiert werden. Wir gewährleisten nur denjenigen Mitarbeitern Zugang zu personenbezogenen Daten, die diesen Zugang für die Arbeit benötigen.

Maßnahmen zur Gewährleistung der Datenqualität

- Qualitätskontrollen: Durchführung regelmäßiger Qualitätskontrollen und Audits der Datensätze, um die Genauigkeit und Zuverlässigkeit der Daten sicherzustellen.
- Standardisierung: Einsatz von Datenstandards und -formaten, um eine konsistente und einheitliche Datenerfassung und -verarbeitung zu gewährleisten.
- Protokollierung von Datenänderungen: Detaillierte Protokollierung aller Datenänderungen, um die Nachverfolgbarkeit und Integrität der Daten zu gewährleisten.

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

- Kundenwünsche: Flexibilität bei der Speicherung der Daten entsprechend den Anforderungen und Wünschen der Kunden, inklusive der Möglichkeit, Daten auf Anfrage des Kunden sicher und vollständig zu löschen.
- Wir speichern nur die Transkripte der Telefonate. Alle weiteren Kategorisierungen sind eine Interpretation des Transkripts. Hardfacts, wie Zeitpunkt, Dauer des Telefonats und Telefonnummer werden ebenfalls gespeichert.

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

- Protokollierung und Dokumentation: Detaillierte Protokollierung und Dokumentation aller Datenverarbeitungsaktivitäten, um Nachvollziehbarkeit und Transparenz zu gewährleisten.
- Zuweisung von Verantwortlichkeiten: Klare Zuweisung von Verantwortlichkeiten für die Datenverarbeitung und -sicherheit innerhalb des Unternehmens, um sicherzustellen, dass alle Mitarbeiter ihre Aufgaben und Pflichten kennen und erfüllen.

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

- Revisionssichere Löschung: Sicherstellung, dass gelöschte Daten revisionssicher und vollständig entfernt werden, ohne Möglichkeit der Wiederherstellung.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Nr. 1: OVH GmbH:

- Anschrift: St. Johanner Str. 41-43, 66111 Saarbrücken, Deutschland
- Kontakt: Datenschutz-Team: datenschutz@ovh.de
- Link AVV: https://www.ovh.de/support/agb/Auftragsverarbeitungsvertrag.pdf und Datenschutz-Informationen https://www.ovh.de/schutz-personenbezogener-daten/dsgvo.xml

Auftragsinhalt:

- Hosting - Cloud-Speicherung und -Verarbeitung: Bereitstellung sicherer und skalierbarer Cloud-Infrastrukturen für die Speicherung und Verarbeitung großer Datenmengen
- Datenbank: Einrichtung und Wartung einer zuverlässigen und performanten Datenbanklösung zur Unterstützung von Geschäftsanwendungen
- Backup: Regelmäßige und automatisierte Backups zur Sicherung von Daten und zur Gewährleistung der Datenwiederherstellung im Notfall

Nr. 2: Twilio Inc.:

- Anschrift: Unter den Linden 10, 10117 Berlin, Deutschland
- Kontakt: Office of the Data Protection Commissioner: info@dataprotection.ie
- Link AVV: https://www.twilio.com/en-us/legal/data-protection-addendum

Auftragsinhalt:

- Dienstleister für Telefonie
- SMS-Dienst
- Erhebung und Speicherung von Anrufdaten: Speicherung von Metadaten wie Telefonnummer, Gesprächsdauer, Zeitpunkt des Gesprächs,…

Nr. 3: Retell AI Inc.:

- Anschrift: San Francisco, California, USA
- Kontakt: founders@retellai.com
- Link Privacy Policy: https://retellai.notion.site/Privacy-Policy-a0bfc26fb3e7429382bbd93837a317f1

Auftragsinhalt:

- RetellAI ist für die Sprachsynthese und Abwicklung des Gesprochenen zuständig, wobei keine Daten gespeichert werden

Nr. 4: Microsoft Ireland Operations Limited (für Azure OpenAI Services)

- **Anschrift**: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
- **Kontakt**: EU Data Protection Officer

- **Link AVV**: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Auftragsinhalt:

- Bereitstellung von OpenAI-Diensten über Microsoft Azure
- KI-gestützte Verarbeitung und Analyse von Textdaten
- Hosting der KI-Dienste innerhalb der EU oder ausgewählter Azure-Regionen gemäß Datenschutzvereinbarung