

Auftragsverarbeitungsvertrag & TOM

Version 2026-09-27 · Stand 27. September 2026

abgeschlossen zwischen

1. ChatSuite GmbH

Technologiepark 12, 33100 Paderborn

(im Folgenden auch kurz „Auftragsverarbeiter“ genannt)

und

2. dem "Verantwortlichen"

(die Vertragsparteien zu 1. und 2. im Folgenden gemeinsam auch kurz die „Vertragsparteien“ oder jeweils für sich die „Vertragspartei“ genannt)

wie folgt:

1. GEGENSTAND, ZWECK UND ANWENDUNGSBEREICH

1.1. Dieser Auftragsverarbeitungsvertrag (nachfolgend auch kurz „AVV“ genannt) 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 sicherstellen.

1.2. Dieser AVV gilt unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

1.3. Gegenstand und Zweck des AVV ist die Durchführung der zwischen Auftragsverarbeiter und Verantwortlichem im Hauptvertrag festgelegten Dienstleistungen. Diese umfassen unter anderem die Speicherung und den Zugriff auf Daten auf einer vom Auftragsverarbeiter betriebenen Plattform.

2. ART DER PERSONENBEZOGENEN DATEN

Im Rahmen der Auftragsverarbeitung werden folgende Arten von personenbezogenen Daten verarbeitet:

- Stammdaten (Name, E-Mail-Adresse, Telefonnummer)
- Kundendaten des Verantwortlichen
- Sonstige vom Verantwortlichen auf die Plattform hochgeladene Daten

3. KATEGORIEN DER BETROFFENEN PERSONEN

Im Rahmen der Auftragsverarbeitung werden personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet:

- Plattformnutzer des Verantwortlichen
- vom Verantwortlichen beauftragte Dienstleister

4. AUSLEGUNG

4.1. Werden in diesem AVV die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

4.2. Dieser AVV ist im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

4.3. Dieser AVV darf nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

5. VORRANG

Im Falle eines Widerspruchs zwischen diesem AVV und den Bestimmungen von mit dem AVV zusammenhängenden Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, hat dieser AVV Vorrang, soweit es die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen betrifft.

6. DAUER DER DATENVERARBEITUNG

Die Dauer der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter korrespondiert mit der Dauer der Datenverarbeitung des Hauptvertrags.

7. PFLICHTEN DER PARTEIEN

7.1. Weisung des Verantwortlichen

7.1.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten (darunter fällt auch die Übermittlung in ein Drittland oder an eine internationale Organisation, die dem Kapitel V der Verordnung (EU) 2016/679 zu entsprechen hat) 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.

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

7.1.3. Die Weisungen des Verantwortlichen ergeben sich aus dem Hauptvertrag und aus seiner Nutzung der Funktionen der Plattform. Darüber hinausgehende Weisungen sind ausschließlich in Textform an info@chatsuite.com zu richten.

7.1.4. Weisungen nach Punkt 7.1.3 Satz 2 sind nur dann für den Auftragsverarbeiter verbindlich, wenn sie in Textform an info@chatsuite.com gerichtet werden. Der Auftragsverarbeiter ist nicht verpflichtet, Weisungen zu befolgen, die auf anderem Weg oder an andere Personen bzw. Stellen gerichtet

werden. Der Verantwortliche stellt den Auftragsverarbeiter von sämtlichen Ansprüchen Dritter aufgrund nicht durchgeführter Weisungen frei, sofern der Verantwortliche die Weisung nicht in Textform an info@chatsuite.com gerichtet hat.

7.1.5. Sofern Weisungen des Verantwortlichen über die im Hauptvertrag festgelegte Leistungspflicht des Auftragsverarbeiters hinausgehen, hat der Auftragsverarbeiter Anspruch auf angemessenes Entgelt.

7.2. Dokumentation und Einhaltung dieses AVV

7.2.1. Die Vertragsparteien müssen die Einhaltung dieses AVV nachweisen können.

7.2.2. Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesem AVV umgehend und in angemessener Weise.

7.2.3. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem AVV festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen AVV fallenden Verarbeitungstätigkeiten einmal jährlich oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Alle zusätzlichen Prüfungen dürfen nur mit vorheriger Zustimmung des Auftragsverarbeiters in Textform und auf Kosten des Verantwortlichen durchgeführt werden.

7.2.4. Prüfungen dürfen den regulären Geschäftsbetrieb des Auftragsverarbeiters nicht beeinträchtigen.

7.2.5. Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen, der jedenfalls kein Wettbewerber des Auftragsverarbeiters sein darf bzw. an dem weder direkt noch indirekt ein Wettbewerber beteiligt sein darf. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

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

7.3. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für die im Hauptvertrag genannten spezifischen Zwecke, sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.4. Sensible Daten

Falls die Verarbeitung personenbezogener 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, wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzliche Garantien an.

8. EINSATZ VON UNTERAUFTRAGSVERARBEITERN

8.1. Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste (Anhang II) aufgeführt sind. Diese Genehmigung umfasst auch die Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, sofern die Übermittlung mit dem Kapitel V der Verordnung (EU) 2016/679 in Einklang steht. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 2 Wochen im Voraus ausdrücklich in Textform 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. Dem Verantwortlichen steht jedoch ein Widerspruchsrecht nur aus wichtigen Gründen zu.

8.2. 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 diesem AVV gelten. Der Auftragsverarbeiter stellt nach bestem Wissen und Gewissen sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesem AVV und gemäß der Verordnung (EU) 2016/679 unterliegt.

8.3. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Umfang und Grenzen dieser Haftung richten sich nach Punkt 12.

9. UNTERSTÜTZUNG DES VERANTWORTLICHEN

9.1. 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.

9.2. 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 Punkten 9.1 und 9.2 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen in angemessener Zeit.

9.3. Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Punkt 9.2 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 (nachfolgend auch kurz „Datenschutz-Folgenabschätzung“ genannt), 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.

9.4. Im Rahmen der Unterstützungspflicht sind die Interessen des Auftragsverarbeiters entsprechend zu berücksichtigen, insbesondere die Größe und wirtschaftliche Situation des Auftragsverarbeiters.

10. 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 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

10.1. 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:

1. 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);
2. 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 personenspezifischen 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;

3. 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.

10.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

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

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2. Name und Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
3. 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.

10.2.2. 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.

10.2.3. Die Meldung gemäß Punkt 10.2.1 ist erfüllt, wenn sie per E-Mail oder auf einem anderen Kommunikationsweg, der üblicherweise mit dem Verantwortlichen genutzt wird, an ein Mitglied der Geschäftsführung des Verantwortlichen, an eine vom Verantwortlichen hierfür benannte Kontaktadresse oder an die E-Mail-Adresse des Inhabers seines ChatSuite-Kontos übermittelt wurde.

11. VERTRAGSDAUER, VERSTÖSSE GEGEN DEN AVV UND BEENDIGUNG DES AVV

11.1. Die Dauer dieses AVV entspricht der Dauer des Hauptvertrags. Mit Beendigung des Hauptvertrags endet automatisch auch dieser AVV, ohne dass es einer gesonderten Kündigung bedarf.

11.2. Falls der Auftragsverarbeiter seinen Pflichten gemäß diesem AVV nicht nachkommt, ist der Verantwortliche berechtigt – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anzuweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diesen AVV einhält oder der AVV beendet ist.

11.3. Der Verantwortliche ist berechtigt, den AVV zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesem AVV betrifft, wenn

1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Punkt 11.2 ausgesetzt hat und die Einhaltung dieses AVV 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 diesen AVV verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesem AVV oder der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

11.4. Der Auftragsverarbeiter ist berechtigt, den AVV zu kündigen, soweit es die Verarbeitung personenbezogener Daten gemäß diesem AVV betrifft, wenn der Verantwortliche auf die Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Punkt 7.1.2 verstoßen.

11.5. Widerspricht der Verantwortliche gemäß Punkt 8.1 einer Änderung der Liste der Unterauftragsverarbeiter, so ist der Auftragsverarbeiter berechtigt, diesen AVV binnen 14 Tagen zu kündigen. Sofern die Erfüllung einer den Auftragsverarbeiter treffenden Pflicht aus dem Hauptvertrag oder aufgrund einer sonstigen rechtlichen Grundlage aufgrund Kündigung bzw. Beendigung dieses AVV nicht mehr zulässig ist und daher vom Auftragsverarbeiter nicht erfüllt wird, stellt der Verantwortliche den Auftragsverarbeiter von den daraus entstehenden Ansprüchen, auch von Ansprüchen Dritter, frei.

11.6. Nach Beendigung des AVV 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. Die Fristen und das Vorgehen, wenn der Verantwortliche keine Wahl trifft, regelt Punkt 11.9. Die Rückgabe der jeweiligen personenbezogenen Daten erfolgt in einem vom Auftragsverarbeiter auszuwählenden üblichen maschinenlesbaren Format. Die Rückgabe bzw. Löschung erfolgt innerhalb angemessener Frist, wobei die aktuelle Auslastung der Ressourcen des Auftragsverarbeiters zu berücksichtigen ist.

11.7. Binnen 7 Tagen nach Rückgabe der personenbezogenen Daten hat der Verantwortliche etwaige Mängel hinsichtlich der Rückgabe in Textform zu rügen oder die ordnungsgemäße Rückgabe der personenbezogenen Daten zu bestätigen. Ist die Rückgabe der personenbezogenen Daten ordnungsgemäß erfolgt, steht dem Verantwortlichen kein Recht zu, gegenüber dem Auftragsverarbeiter Ansprüche wegen nicht ordnungsgemäßer Rückgabe der personenbezogenen Daten oder eine diesbezügliche Einrede geltend zu machen.

11.8. Bis zur Löschung oder Rückgabe der personenbezogenen Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieses AVV.

11.9. Der Auftragsverarbeiter hält die personenbezogenen Daten nach Beendigung noch 30 Tage bereit. Verlangt der Verantwortliche innerhalb dieser Frist in Textform die Rückgabe gemäß Punkt 11.6, gibt der Auftragsverarbeiter die personenbezogenen Daten zurück. Nach Ablauf dieser Frist, im Falle einer Rückgabe jedoch nicht vor Ablauf der Frist gemäß Punkt 11.7, löscht der Auftragsverarbeiter die personenbezogenen Daten und bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

11.10. Die Löschverpflichtung nach diesem Punkt 11 gilt auch dann als erfüllt, wenn die Löschung von Backups oder anderen Sicherungen erst nach Ablauf der Frist gemäß Punkt 11.9 erfolgt, sofern durch regelmäßige Überschreibung der Backups oder der anderen Sicherungen eine Löschung spätestens 30 Tage nach Ablauf dieser Frist sichergestellt ist und eine Löschung innerhalb der Frist gemäß Punkt 11.9 unverhältnismäßig wäre.

12. HAFTUNG

Für die Haftung der Vertragsparteien gilt der Abschnitt „Haftung“ der Allgemeinen Geschäftsbedingungen (AGB) des Auftragsverarbeiters in der bei Vertragsschluss vereinbarten Fassung; dies gilt auch für die Einstandspflicht nach Punkt 8.3. Die Haftung gegenüber betroffenen Personen nach Art. 82 der Verordnung (EU) 2016/679 bleibt unberührt.

13. WEITERVERARBEITUNG DER PERSONENBEZOGENEN DATEN

Die Weiterleitung der im Rahmen dieses AVV verarbeiteten personenbezogenen Daten ist zulässig, sofern ein Kompatibilitätstest im Sinne von Art. 6 Abs. 4 DSGVO durchgeführt wird und eine Weiterverarbeitung gemäß Art. 6 Abs. 4 DSGVO zulässig ist.

14. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

14.1. Der Auftragsverarbeiter ergreift mindestens die in Anhang I 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 auch kurz „Verletzung des Schutzes personenbezogener Daten“ genannt). 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.

14.2. 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 AVV 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.

15. SCHLUSSBESTIMMUNGEN

15.1. Die Anhänge I bis II bilden einen integralen Bestandteil dieses AVV.

15.2. Änderungen oder Ergänzungen dieses AVV bedürfen der Textform.

15.3. Keine der Vertragsparteien ist berechtigt, ihre Rechte aus diesem AVV an einen Dritten abzutreten, sofern in diesem Vertrag nicht ausdrücklich Abweichendes bestimmt ist.

15.4. Auch die längere Nichtausübung eines Rechts führt nicht zum Rechtsverlust und ist nicht als Verzicht zu werten.

15.5. Sollte eine Bestimmung dieses Vertrages nichtig, ungültig, unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen dieses Vertrages hiervon unberührt. Anstelle der nichtigen, ungültigen, unwirksamen oder undurchführbaren Bestimmung gilt diejenige wirksame bzw. durchführbare Bestimmung als vereinbart, die dem mit der nichtigen, ungültigen, unwirksamen oder undurchführbaren Bestimmung verfolgten wirtschaftlichen Zweck möglichst nahekommt. Entsprechendes gilt für die ergänzende Vertragsauslegung im Fall von Lücken dieses Vertrags.

15.6. Dieser AVV unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

15.7. Ist der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen oder hat er keinen allgemeinen Gerichtsstand in Deutschland, ist ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV Paderborn. Der Auftragsverarbeiter kann auch am allgemeinen Gerichtsstand des Verantwortlichen klagen.

Anhang I – Technische und organisatorische Maßnahmen (TOM)

1. GRUNDSÄTZLICHE MASSNAHMEN

1.1. Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

1.2. Der Auftragsverarbeiter hat ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogen und mindestens halbjährlich evaluiert wird, eingerichtet. Darüber hinaus besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

1.3. Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen. Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).

1.4. Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung. Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.

1.5. Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virens Scanner und Firewalls.

1.6. Hardware kann remote gesperrt und gelöscht werden. Beim Ausscheiden von Beschäftigten wird der zentrale Account gesperrt und damit auch alle Zugriffe auf Server und Tools.

1.7. Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebensächlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

2. MASSNAHMEN ZUR PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG VON PERSONENBEZOGENEN DATEN GEM. ART. 32 ABS. 1 LIT. A DSGVO

Der Auftragsverarbeiter verwendet Standardverschlüsselungsmethoden, um alle personenbezogenen Daten zu schützen.

3. MASSNAHMEN ZUR SICHERSTELLUNG DER LAUFENDEN VERTRAULICHKEIT GEM. ART. 32 ABS. 1 LIT. B DSGVO

Der Auftragsverarbeiter ergreift Maßnahmen zur Gewährleistung der ständigen Vertraulichkeit. Dazu gehören insbesondere Maßnahmen zur physischen und elektronischen Zugangskontrolle. Diese Maßnahmen gewährleisten den Schutz gegen unbefugte oder unrechtmäßige Verarbeitung und gegen zufällige Zerstörung, Verlust oder Beschädigung.

3.1. Physische Zugangskontrolle

- Im Büro des Auftragsverarbeiters befinden sich keine Server-Systeme.
- Der Zutritt zum Betriebsgelände ist nur Mitarbeitern des Auftragsverarbeiters gestattet.
- Das Betriebsgelände bzw. die Büroräumlichkeiten sind mit Sicherheitsschlössern verschlossen.
- Der Auftragsverarbeiter nutzt Server der folgenden Unterauftragsverarbeiter:
 - Siehe Anhang II.

3.2. Elektronische Zugangskontrolle

- Der Zugang zu personenbezogenen Daten wird nur einer begrenzten Gruppe von Mitarbeitern gewährt.
- Der Zugang zu personenbezogenen Daten erfordert eine Benutzer-ID und ein Passwort sowie eine Zwei-Faktor-Authentifizierung und ist durch HTTPS und SSL gesichert.
- Benutzerkonten/IDs werden sofort deaktiviert/gelöscht, wenn Mitarbeiter das Unternehmen verlassen.
- Passwörter werden nicht im Klartext gespeichert oder unverschlüsselt übertragen.
- Passwörter sind regelmäßig zu ändern.
- Benutzer- und Benutzergruppenverwaltungssystem

3.3. Zugriffskontrolle

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten innerhalb des Systems durch Standard-Berechtigungsprofile auf „need to know-Basis“
- Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen,
- periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten zum Server

4. MASSNAHMEN ZUR SICHERSTELLUNG DER LAUFENDEN INTEGRITÄT GEM. ART. 32 ABS. 1 LIT. B DSGVO

Der Auftragsverarbeiter ergreift Maßnahmen, um die ständige Integrität zu gewährleisten. Dazu gehören Maßnahmen zur Kontrolle der Eingabe, zur Kontrolle der Übermittlung personenbezogener Daten und ganz allgemein zum Schutz personenbezogener Daten vor unrechtmäßiger oder unzulässiger Verarbeitung.

4.1. Kontrolle der Übermittlung

Maßnahmen, die sicherstellen, dass personenbezogene Daten während der elektronischen Übermittlung oder während des Transports oder der Speicherung auf Datenträgern nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können, und dass es möglich ist, zu überprüfen und festzustellen, an welche Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden sollen.

- VPN
- Protokollierung von Zugriffen und Abrufen
- verschlüsselte Verbindungen wie sftp, https und sichere Cloudspeicher
- sichere drahtlose Netzwerke (WLAN), die mit WPA-2 verschlüsselt sind.

4.2. Eingabekontrolle

Maßnahmen, die sicherstellen, dass im Nachhinein überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus ihnen entfernt wurden

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Grundlage eines Berechtigungskonzepts

5. MASSNAHMEN ZUR SICHERSTELLUNG DER STÄNDIGEN VERFÜGBARKEIT UND BELASTBARKEIT GEM. ART. 32 ABS. 1 LIT. B DSGVO

Der Auftragsverarbeiter trifft Maßnahmen, um die ständige Verfügbarkeit und Belastbarkeit zu gewährleisten. Dazu gehören auch Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen versehentliche Zerstörung oder Verlust geschützt sind.

Der Auftragsverarbeiter betreibt keine Serversysteme. Serversysteme werden von externen Unternehmen betrieben (siehe Anhang II.). Um die ständige Verfügbarkeit und Ausfallsicherheit zu gewährleisten, nutzt der Auftragsverarbeiter mehrere Serversysteme.

6. MASSNAHMEN ZUR SICHERSTELLUNG DER WIEDERHERSTELLBARKEIT GEM. ART. 32 ABS. 1 LIT. C DSGVO

Der Auftragsverarbeiter trifft Maßnahmen, um sicherzustellen, dass die Verfügbarkeit personenbezogener Daten und der Zugang zu ihnen, im Falle eines physischen oder technischen Zwischenfalls rasch wiederhergestellt werden können.

- Tägliche Datensicherung
- Redundante Speicherung
- Überwachung und Berichterstattung
- Wiederherstellungsplan

7. MASSNAHMEN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG GEM. ART. 32 ABS. 1 LIT. D DSGVO

Der Auftragsverarbeiter ergreift Maßnahmen zur Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen.

- Regelmäßige Überprüfung
- Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig durchgeführt
- Die technischen und organisatorischen Maßnahmen werden regelmäßig aktualisiert
- Zentrale Dokumentation aller Datenschutzbestimmungen mit Zugang für Mitarbeiter
- Auswertung von Meldungen von Kunden
- Auswertung von Meldungen über besondere Vorkommnisse
- Mitarbeiterschulungen zum Umgang mit IT, IT-Sicherheit und Datenschutzmaßnahmen
- Formalisierter Prozess für Auskunftersuchen von betroffenen Personen ist vorhanden
- Interner Beauftragter für Informationssicherheit ernannt

Anhang II – Unterauftragsverarbeiter

1. Server Infrastruktur

Diese Art von Dienst dient dazu, die Infrastruktur auf dedizierten Servern auszulagern.

IONOS SE
Elgendorfer Straße 57
56410 Montabaur, Deutschland

2. Webspeicher

Diese Art von Dienst dient dazu, die Auftragsdaten in Microsoft Azure Blob-Containern zu speichern.

Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park
Dublin D18 P521, Irland

3. Einsatz von KI

Diese Art von Dienst dient dazu, die Auftragsdaten mittels KI zu verarbeiten. Die KI-Verarbeitung erfolgt ausschließlich über Microsoft Azure. Hierfür werden regionale Azure-Dienste innerhalb der Europäischen Union sowie die europäische Azure-Datenzone (EU Data Zone) genutzt. Die EU Data Zone umfasst neben EU-Mitgliedstaaten auch EFTA-Staaten, insbesondere Norwegen und die Schweiz.

Die eingesetzten KI-Dienste werden mit Zero Data Retention betrieben. Die übermittelten Eingaben und die erzeugten Ausgaben werden beim KI-Dienst nicht dauerhaft gespeichert und nicht zum Training der KI-Modelle verwendet. Dies betrifft die Verarbeitung beim KI-Dienst; die für die vereinbarten Leistungen erforderliche Speicherung von Auftragsdaten in ChatSuite bleibt hiervon unberührt.

Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park
Dublin D18 P521, Irland

4. WhatsApp-Kommunikation

Diese Art von Dienst dient dazu, Nachrichten in WhatsApp-Gruppen und WhatsApp-Einzelchats zu übertragen.

WhatsApp Ireland Limited
Merrion Road
Dublin 4, D04 X2K5, Irland

WhatsApp wird über die vom Verantwortlichen eingebrachten WhatsApp-Konten genutzt. Die Anbindung erfolgt über eine WhatsApp-Web-Sitzung (verknüpftes Gerät) der jeweiligen Rufnummer; die offizielle WhatsApp Business Plattform (Cloud API) von Meta wird nicht genutzt. Die

datenschutzrechtliche Rolle von WhatsApp richtet sich nach den Bedingungen, die für das jeweilige WhatsApp-Konto gelten.

5. E-Mail-Versand

Diese Art von Dienst dient dazu, Benachrichtigungs-, Konto- und Sicherheits-E-Mails an Nutzer der Plattform sowie vom Verantwortlichen in Automationen eingerichtete E-Mails (einschließlich Anhängen) an dessen Kunden und weitere Empfänger zu versenden.

IONOS SE
Elgendorfer Straße 57
56410 Montabaur, Deutschland

6. SMS-Versand

Diese Art von Dienst dient dazu, vom Verantwortlichen veranlasste Einladungs-SMS mit dem Link zu einer WhatsApp-Gruppe an dessen Kunden zu versenden und vor dem Versand zu prüfen, ob die Rufnummer SMS empfangen kann. Übermittelt werden die Rufnummer und der Text der SMS.

Twilio Ireland Limited
70 Sir John Rogerson's Quay
Dublin 2, D02 R296, Irland

Twilio verarbeitet die Daten auch in den USA. Die Übermittlung stützt sich auf die Zertifizierung der Twilio Inc. nach dem EU-U.S. Data Privacy Framework sowie auf die EU-Standardvertragsklauseln der Datenschutzvereinbarung von Twilio.