Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

Die vorliegende Vereinbarung zur Auftragsverarbeitung („AVV“) wird zwischen der

(nachfolgend „Auftraggeber“ oder „Verantwortlicher“),
und
der **Siteware GmbH**, Am Weilsberg 11, 51789 Lindlar (nachfolgend „Auftragsverarbeiter“ oder „Siteware“)

geschlossen.

1. Präambel

Siteware ist ein DSGVO-konformes SaaS-System, das speziell dazu entwickelt wurde, künstliche Intelligenz in verschiedensten Branchen nutzbar zu machen – und das ohne tiefgreifende Vorkenntnisse in KI-Technologien. Mittels spezialisierter KI-Agenten werden wiederkehrende Tätigkeiten automatisiert. Durch nahtlose Integration von Modellen wie ChatGPT, Google Gemini, Anthropic Claude und Bildgeneratoren wird ein flexibles, modellunabhängiges Angebot bereitgestellt. Dank der hohen Integrationsfähigkeit ist Siteware in der Lage, sich an spezifische Anforderungen unterschiedlicher Branchen anzupassen.

Siteware erbringt für den Verantwortlichen Leistungen im Zusammenhang mit der Nutzung von Siteware. Dies umfasst insbesondere die Bereitstellung von KI-Werkzeugen, Chatbots und Conversational Chatbots in Form von SaaS-Diensten sowie damit verbundene unterstützende Tätigkeiten. Der Verantwortliche überträgt dem Auftragsverarbeiter hierzu die Verarbeitung personenbezogener Daten im Sinne der EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „DSGVO“) sowie des Bundesdatenschutzgesetzes (BDSG) in der jeweils geltenden Fassung.

Um den Anforderungen des Art. 28 DSGVO gerecht zu werden und die Einhaltung weiterer nationaler und internationaler Datenschutzvorschriften sicherzustellen, vereinbaren die Parteien die nachfolgenden Regelungen. Diese sollen gewährleisten, dass die **Verarbeitung personenbezogener Daten** ausschließlich nach den Weisungen des Verantwortlichen erfolgt und den geltenden **Datenschutz- und Datensicherheitsanforderungen** entspricht.

Im Rahmen dieser Vereinbarung finden zusätzlich die Bestimmungen folgender Rechtsquellen Anwendung, sofern sie einschlägig sind und auf die Leistungen des Auftragsverarbeiters zutreffen:

EU-Datenschutz-Grundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG), ePrivacy-Richtlinie bzw. ePrivacy-Verordnung, UK GDPR, Swiss FADP, Standardvertragsklauseln (SCC), Binding Corporate Rules (BCR), Leitlinien des Europäischen Datenschutzausschusses (EDSA/EDPB), Branchenspezifische Anforderungen, Sonstige nationale Datenschutzgesetze

GESONDERTE HINWEISE

Falls die in diesem Vertrag näher zu konkretisierenden Dienstleistungen oder Datenverarbeitungen weitere länderspezifische Anforderungen oder Branchenvorschriften betreffen, werden diese in relevanten Anlagen geregelt.

Beide Parteien versichern, die Vorgaben dieser Vereinbarung gewissenhaft zu befolgen und die Rechte der betroffenen Personen im Hinblick auf deren personenbezogene Daten zu wahren.

2. Definitionen

2.1 **Verantwortlicher (Controller)**
Als „Verantwortlicher“ wird die Stelle bezeichnet, die im Sinne der DSGVO, insbesondere nach Art. 4 Nr. 7 DSGVO, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Im Rahmen dieses Vertrags ist dies der Auftraggeber.

2.2 **Auftragsverarbeiter (Processor)**
„Auftragsverarbeiter“ im Sinne der DSGVO, insbesondere nach Art. 4 Nr. 8 DSGVO, ist die Siteware GmbH, Am Weilsberg 11, 51789 Lindlar, die personenbezogene Daten im Auftrag des Verantwortlichen und nach dessen Weisungen verarbeitet.

2.3 **Personenbezogene Daten**
„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (gemäß Art. 4 Nr. 1 DSGVO), wie etwa Name, E-Mail-Adresse, Telefonnummer, Anschrift, Zahlungsinformationen, Geburtsdatum, IP-Adresse, Nutzungsdaten, Cookie-Daten

2.4 **Betroffene Person**
„Betroffene Person“ ist jede natürliche Person, deren personenbezogene Daten verarbeitet werden (Art. 4 Nr. 1 DSGVO). Hierzu können Mitarbeiter, Kunden, Lieferanten, Website-Besucher, Newsletter-Abonnenten, Bewerber, Interessenten gehören.

2.5 **Unterauftragsverarbeiter (Subprozessor)**
„Unterauftragsverarbeiter“ oder „Subprozessor“ ist ein weiterer Auftragsverarbeiter, den der Haupt-Auftragsverarbeiter zur Erfüllung seiner vertraglichen Leistungen beauftragt. Der Verantwortliche muss der Beauftragung von Unterauftragsverarbeitern grundsätzlich zustimmen (Art. 28 Abs. 2 und 4 DSGVO). Eine aktuelle Liste sämtlicher Unterauftragsverarbeiter ist der Anlage Unterauftragsverarbeiter zu entnehmen.

2.6 **Technische und organisatorische Maßnahmen (TOM)**
„Technische und organisatorische Maßnahmen“ sind Sicherheitsvorkehrungen gemäß Art. 32 DSGVO, die Siteware als Auftragsverarbeiter zum Schutz der verarbeiteten personenbezogenen Daten implementiert. Eine Übersicht dieser Maßnahmen ist in der Anlage TOM enthalten.

2.7 **Weisung**
„Weisung“ bezeichnet jede schriftliche oder in dokumentierter Form erteilte Anleitung des Verantwortlichen an den Auftragsverarbeiter im Zusammenhang mit der Verarbeitung personenbezogener Daten (Art. 29 DSGVO). Weisungen müssen dem vertraglich vereinbarten Verfahren zur Weisungserteilung entsprechen.

2.8 **Meldepflichten**
„Meldepflichten“ bezeichnen die Verpflichtung, im Falle einer Verletzung des Schutzes personenbezogener Daten („Datenpanne“) den Verantwortlichen unverzüglich zu informieren und gegebenenfalls die zuständige Datenschutzaufsichtsbehörde sowie die betroffenen Personen nach Art. 33 und 34 DSGVO zu benachrichtigen.

2.9 **Drittländer**
„Drittländer“ sind Staaten außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR), für welche grundsätzlich die Vorgaben zum internationalen Datenverkehr gem. Kapitel V DSGVO gelten. Transfers in solche Länder dürfen nur auf Grundlage von Standardvertragsklauseln oder Angemessenheitsbeschlüssen erfolgen.

3. Gegenstand und Dauer der Verarbeitung

3.1 **Gegenstand der Datenverarbeitung**
Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich für die Nutzung von Siteware. Dies umfasst insbesondere die Bereitstellung von KI-Werkzeugen, Chatbots und Conversational Chatbots in Form von SaaS-Diensten sowie damit verbundene unterstützende Tätigkeiten. Die Verarbeitung erfolgt in Übereinstimmung mit den Bestimmungen dieses Vertrags, den Vorgaben der DSGVO sowie den anwendbaren nationalen und internationalen Datenschutzvorschriften.

3.2 **Art und Zweck der Verarbeitung**

- **Art der Daten:** Es werden ausschließlich Daten verarbeitet, die für die Erbringung der vereinbarten Leistung erforderlich sind, insbesondere z. B. Kontaktdaten, Inhaltsdaten und Protokolldaten.
- **Zweck der Verarbeitung:** Die Verarbeitung personenbezogener Daten dient der Kommunikation, der automatisierten Erstellung von Texten, der Datenanalyse und der Protokollierung von Vorgängen und erfolgt dabei nach den Weisungen des Verantwortlichen (siehe Kapitel Weisungsrecht).

3.3 **Kategorien betroffener Personen**
Zu den betroffenen Personen zählen in der Regel Mitarbeiter:innen, Kunden und Lieferanten, deren personenbezogene Daten im Rahmen der o. g. Leistungen erhoben, gespeichert oder auf sonstige Weise verarbeitet werden.

3.4 **Umfang der Verarbeitung**
Der Umfang der Datenverarbeitung beschränkt sich auf das zur Erfüllung des Vertragszwecks notwendige Maß. Siteware ist nicht berechtigt, die erhaltenen personenbezogenen Daten für eigene Zwecke zu verwenden oder Dritten ohne Weisung des Verantwortlichen zugänglich zu machen, sofern keine gesetzliche Verpflichtung dazu besteht.

3.5 **Dauer der Verarbeitung**
Die Verarbeitung erfolgt für die Dauer der Nutzung von Siteware. Nach Beendigung des Vertrags und Ablauf etwaiger gesetzlicher Aufbewahrungsfristen sind die personenbezogenen Daten nach Wahl des Verantwortlichen unverzüglich zu löschen oder zurückzugeben (siehe hierzu auch Kapitel **Beendigung des Vertrags**). Sofern es für die Erfüllung gesetzlicher Pflichten erforderlich ist, kann die Verarbeitung – in Abstimmung mit dem Verantwortlichen – über die Vertragslaufzeit hinausgehen.

3.6 **Laufzeit und Kündigung**
Dieser Vertrag tritt mit der Unterzeichnung durch beide Parteien in Kraft und läuft bis zum Ende der Nutzung von SIteware, sofern keine abweichenden Regelungen vereinbart wurden. Die Möglichkeit einer außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

4. Technische und organisatorische Maßnahmen (TOM)

4.1 **Allgemeine Anforderungen**
Der Auftragsverarbeiter stellt sicher, dass sämtliche gemäß Art. 32 DSGVO geforderten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten umgesetzt werden. Diese Maßnahmen orientieren sich an den branchenüblichen Standards und werden in regelmäßigen Abständen auf ihre Wirksamkeit überprüft und, falls erforderlich, angepasst.

4.2 **Beschreibung der einzelnen Maßnahmen**
Eine detaillierte Übersicht der implementierten technischen und organisatorischen Maßnahmen ist in Anlage TOM aufgeführt und umfasst u. a. folgende Bereiche:

- **Zugangs- und Zutrittskontrolle:**
  - Sicherung der Räumlichkeiten und Serverräume vor unbefugtem Zutritt.
  - Einrichtung von Schließanlage oder elektronische Zugangskarten.
- **Zugriffskontrolle:**
  - Vergabe von Rollen- und Berechtigungskonzepten.
  - z. B. Multi-Faktor-Authentifizierung.
- **Weitergabekontrolle:**
  - Protokollierung jeglicher Datenübermittlungen an Dritte.
  - Nutzung von TLS/SSL für Datenübermittlungen.
- **Eingabekontrolle:**
  - Protokollierung von Dateneingaben und -änderungen.
  - Nachweisbarkeit aller Änderungen durch Logging und Monitoring
- **Auftragskontrolle:**
  - Verarbeitung ausschließlich nach Weisung des Verantwortlichen.
  - Implementierung geeigneter Prozesse zur Weisungserteilung und Umsetzung
- **Verfügbarkeitskontrolle:**
  - Backup- und Restorekonzepte zur Sicherung der Daten.
- **Trennungsgebot:**
  - Physische oder logische Trennung von Daten, die zu unterschiedlichen Zwecken verarbeitet werden.
- **Pseudonymisierung und Verschlüsselung:**
  - Soweit möglich, Verfahren zur Anonymisierung und Pseudoanonymisierung
  - Durchgängige Verschlüsselung.

4.3 **Dokumentation und Nachweisführung**
Der Auftragsverarbeiter dokumentiert alle getroffenen technischen und organisatorischen Maßnahmen und die regelmäßigen Kontrollen ihrer Wirksamkeit. Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen relevante Nachweise zur Verfügung, damit dieser seine gesetzlichen Pflichten aus Art. 28 DSGVO sowie weiteren Datenschutzbestimmungen erfüllen kann.

4.4 **Fortlaufende Überprüfung und Anpassung**
Der Auftragsverarbeiter verpflichtet sich, die in Anlage TOM beschriebenen Schutzmaßnahmen regelmäßig zu überprüfen und an den aktuellen Stand von Technik und Recht anzupassen. Änderungen werden unverzüglich dokumentiert und dem Verantwortlichen innerhalb einer Woche schriftlich oder elektronisch mitgeteilt.

4.5 **Vertraulichkeit und Sensibilisierung**
Der Auftragsverarbeiter stellt sicher, dass alle Personen, die Zugang zu personenbezogenen Daten haben oder in deren Verarbeitung eingebunden sind, Verpflichtungen zur Vertraulichkeit unterworfen sind und entsprechende Schulungen zu Datenschutz- und Datensicherheitsmaßnahmen erhalten. Die Verpflichtung der Mitarbeitenden zur Vertraulichkeit besteht auch nach Beendigung ihrer Tätigkeit fort.

4.6 **Meldepflichten bei Sicherheitsvorfällen**
Bei einer Verletzung des Schutzes personenbezogener Daten (Datenpanne) informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich gemäß Art. 33 und Art. 34 DSGVO.. Die weitere Vorgehensweise wird mit dem Verantwortlichen abgestimmt, insbesondere was die Benachrichtigung der zuständigen Datenschutzaufsichtsbehörde(n) und ggf. der betroffenen Personen anbelangt.

5. Weisungsrecht des Verantwortlichen

5.1 **Allgemeine Weisungserteilung**
Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich auf Grundlage der vereinbarten Weisungen des Verantwortlichen und im Rahmen dieses Auftragsverarbeitungsvertrags (AVV). Der Verantwortliche behält sich das Recht vor, Art und Umfang der Weisungen jederzeit zu präzisieren oder zu ändern, sofern dies unter Wahrung datenschutzrechtlicher Vorgaben erfolgt.

5.2 **Form und Dokumentation der Weisungen**
Weisungen sind grundsätzlich schriftlich oder elektronisch zu erteilen und vom Auftragsverarbeiter in geeigneter Weise zu dokumentieren. Mündliche Weisungen sind zulässig, sofern sie umgehend in schriftlich festgehalten werden und für beide Parteien nachvollziehbar sind.

5.3 **Änderungen und Ergänzungen von Weisungen**
Der Auftragsverarbeiter ist verpflichtet, Änderungen oder Ergänzungen von Weisungen umzusetzen, sofern diese die Einhaltung der DSGVO und die Machbarkeit erfüllen. Entstehen dem Auftragsverarbeiter durch zusätzliche Weisungen erhebliche Kosten oder Mehraufwendungen, wird der Auftragsverarbeiter den Verantwortlichen vorab schriftlich oder elektronisch darüber informieren und die weitere Vorgehensweise abstimmen.

5.4 **Rechtswidrige Weisungen**
Sollte der Auftragsverarbeiter der Auffassung sein, dass eine Weisung des Verantwortlichen gegen geltende datenschutzrechtliche Bestimmungen oder diesen Vertrag verstößt, hat er den Verantwortlichen unverzüglich schriftlich oder elektronisch darüber zu informieren. Der Auftragsverarbeiter ist berechtigt, die Umsetzung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder angepasst wurde.

5.5 **Konsequenzen bei Verstößen**
Handelt der Auftragsverarbeiter entgegen den Weisungen des Verantwortlichen oder ohne eine Weisung, haftet er gegenüber dem Verantwortlichen für sämtliche daraus resultierenden Schäden gemäß den Bestimmungen zur Haftungsregelung dieses Vertrags. Der Auftragsverarbeiter übernimmt die Verantwortung für alle Folgen, die sich aus einer von ihm ohne Weisung oder entgegen einer Weisung vorgenommenen Verarbeitung ergeben.

5.6 **Nachweis der Weisungserfüllung**
Der Auftragsverarbeiter legt dem Verantwortlichen auf Anfrage entsprechende Nachweise vor, aus dem hervorgeht, inwiefern Weisungen eingehalten und korrekt umgesetzt wurden. Auf diese Weise kann der Verantwortliche die ordnungsgemäße Auftragsdurchführung überprüfen und sicherstellen, dass die Vorgaben aus Art. 28 DSGVO sowie weiteren Datenschutzvorschriften eingehalten werden.

6. Unterauftragsverhältnisse (Subprozessoren)

6.1 **Einsatz von Unterauftragsverarbeitern**
Der Auftragsverarbeiter ist berechtigt, zur Erfüllung seiner vertraglichen Pflichten gegenüber dem Verantwortlichen Unterauftragsverarbeiter (Subprozessor) einzusetzen, sofern der Verantwortliche zuvor seine Zustimmung erteilt hat. Eine aktuelle und vollständige Liste sämtlicher vom Auftragsverarbeiter eingesetzter Subprozessoren wird in Anlage Unterauftragsverarbeiter geführt und dem Verantwortlichen auf Anfrage zur Verfügung gestellt.

6.2 **Zulässigkeit und Genehmigung**

- **Vorherige Zustimmung:** Der Auftragsverarbeiter holt vor der Beauftragung eines neuen oder der Ersetzung eines bestehenden Subprozessors die Zustimmung des Verantwortlichen ein. Diese Zustimmung kann schriftlich oder elektronisch erfolgen.
- **Widerspruchsrecht:** Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund gegen die Einbindung oder den Wechsel des Subprozessors innerhalb von 30 Tagen nach entsprechender Mitteilung durch den Auftragsverarbeiter widersprechen.

6.3 **Vertragliche Verpflichtungen der Subprozessoren**
Der Auftragsverarbeiter schließt mit jedem Subprozessor eine schriftliche Vereinbarung ab, die mindestens den Anforderungen dieses AVV und des Art. 28 DSGVO entspricht. Darin wird insbesondere sichergestellt, dass:

- der Subprozessor personenbezogene Daten ausschließlich auf Weisung des Auftragsverarbeiters (und mittelbar auf Weisung des Verantwortlichen) verarbeitet,
- der Subprozessor angemessene technische und organisatorische Maßnahmen (TOM) einhält, die den Vorgaben dieses Vertrags entsprechen,
- die erforderlichen Haftungs- und Sorgfaltspflichten zwischen Auftragsverarbeiter und Subprozessor geregelt sind.

6.4 **Haftung und Verantwortlichkeiten**
Der Auftragsverarbeiter haftet für das Verhalten seiner Subprozessoren gegenüber dem Verantwortlichen wie für eigenes Verhalten. Dies umfasst alle Verstöße gegen Datenschutzvorschriften oder Weisungen des Verantwortlichen, die sich aus dem Tätigwerden der Subprozessoren ergeben. Die Haftungsgrenzen und Schadensersatzregelungen des vorliegenden Vertrags finden auch Anwendung für Ansprüche, die aufgrund fehlerhaften Verhaltens eines Subprozessors entstehen.

6.5 **Information des Verantwortlichen**
Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über alle wesentlichen Änderungen in Bezug auf seine Subprozessoren, insbesondere über:

- **Beabsichtigte Neueinsetzung oder Ersetzung** eines Subprozessors,
- **Änderungen der vertraglichen Konditionen** mit einem Subprozessor, sofern sie datenschutzrechtliche Auswirkungen haben,
- **Sicherheitsvorfälle** oder datenschutzrechtliche Verstöße, die beim Subprozessor aufgetreten sind und die Verarbeitung personenbezogener Daten des Verantwortlichen unmittelbar betreffen.

6.6 **Kontrolle der Subprozessoren**
Der Auftragsverarbeiter gewährleistet, dass er sich regelmäßig von der Prozessqualität seiner Subprozessoren überzeugt. Auf Verlangen des Verantwortlichen wird der Auftragsverarbeiter Art und Umfang der Kontrolle dokumentieren und dem Verantwortlichen zur Verfügung stellen. Sofern der Verantwortliche aus wichtigem Grund eine direkte Kontaktaufnahme mit dem Subprozessor wünscht, stimmt der Auftragsverarbeiter dies im Einvernehmen mit allen beteiligten Parteien ab, um sicherzustellen, dass keine vertraulichen Informationen Dritter preisgegeben werden und geltende Datenschutzbestimmungen eingehalten werden.

Alle an Siteware angebundenen KI-Modelle verwenden die Daten nicht zu internen Trainingszwecken und speichern die Daten nicht dauerhaft.

6.7 **Speicherung und Löschung**
Alle an Siteware angebundenen KI-Modelle verwenden die Daten nicht zu internen Trainingszwecken und speichern die Daten nicht dauerhaft. Alle Sprachaufnahmen und Transkriptionen werden ausschließlich für den jeweiligen Anwendungsfall verarbeitet, verschlüsselt gespeichert und nach definierten Löschfristen entfernt, um den strengen Anforderungen der DSGVO gerecht zu werden.

6.8 **Datenübermittlung und -verarbeitung über die Siteware API**
Sofern Kooperationspartner die Siteware API in ihre Software integrieren, erfolgt der Zugriff auf die angeschlossenen KI-Modelle unter strikter Einhaltung der hohen Datenschutzstandards, die auch im Zusammenspiel mit den Modellbetreibern gelten. Kundendaten, die über die API übermittelt werden, werden ausschließlich zur Erfüllung der vertraglich vereinbarten Leistungen genutzt und dürfen weder dauerhaft gespeichert noch zur nachträglichen Modellierung oder zum Training der KI-Modelle herangezogen werden. Die beteiligten Modellbetreiber haben vertraglich zugesichert, dass sämtliche übermittelte Daten unmittelbar nach der Verarbeitung gelöscht werden bzw. nur temporär und in pseudonymisierter Form zur Erfüllung technischer Prozesse vorgehalten werden.Durch den verschlüsselten Datenaustausch wird sichergestellt, dass sämtliche Datenübermittlungen und -verarbeitungen lückenlos, dokumentiert und den geltenden Datenschutzvorgaben unterworfen werden. Somit profitieren unsere Kooperationspartner von den hohen Sicherheitsstandards und der Datenschutzkonformität, die Siteware und die angeschlossenen KI-Modelle gewährleisten.

7. Pflichten des Auftragsverarbeiters

7.1 **Verarbeitung nach Weisung**
Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich im Rahmen der vereinbarten Weisungen des Verantwortlichen zu verarbeiten und die Pflichten aus diesem Vertrag sowie den einschlägigen Datenschutzbestimmungen einzuhalten. Der Auftragsverarbeiter verwendet die überlassenen Daten nicht für eigene Zwecke und legt sie Dritten nicht ohne Weisung oder eine gesetzliche Verpflichtung offen.

7.2 **Vertraulichkeit und Schulung**

- **Verpflichtung zur Vertraulichkeit:** Alle Personen, die beim Auftragsverarbeiter oder einem Subprozessor mit der Verarbeitung personenbezogener Daten befasst sind, werden der Verpflichtung zur Vertraulichkeit unterworfen. Diese Verpflichtung besteht auch nach Beendigung der jeweiligen Tätigkeit fort.
- **Schulung der Mitarbeitenden:** Der Auftragsverarbeiter sorgt dafür, dass das mit der Verarbeitung betraute Personal regelmäßig Datenschutz- und Sicherheitsschulungen durchläuft, um die aktuellen datenschutzrechtlichen Anforderungen sowie die internen Prozesse und Sicherheitsmaßnahmen zu kennen und befolgen zu können.

7.3 **Unterstützung bei Betroffenenrechten**
Der Auftragsverarbeiter unterstützt den Verantwortlichen in zumutbarem Umfang bei der **Bearbeitung von Anfragen betroffener Personen** gemäß Kapitel III DSGVO (insbesondere Art. 12–22 DSGVO, z. B. Auskunfts-, Lösch- oder Berichtigungsverlangen). Hierzu gehören insbesondere:

- **Weiterleitung** von Anfragen an den Verantwortlichen, sofern diese unmittelbar beim Auftragsverarbeiter eingehen,
- **Bereitstellung** der notwendigen Informationen und Daten, damit der Verantwortliche seiner Pflicht zur Beantwortung der Betroffenenrechte nachkommen kann,
- **Umsetzung** von Anordnungen des Verantwortlichen (z. B. Datenlöschungen, Einschränkungen der Verarbeitung), sofern sie sich im Rahmen dieses Vertrags und der gesetzlichen Vorgaben bewegen.

7.4 **Unterstützung bei Melde- und Benachrichtigungspflichten**
Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, sobald ihm Anhaltspunkte für eine Datenschutzverletzung (Art. 33, 34 DSGVO) vorliegen. Er unterstützt den Verantwortlichen bei allen sich daraus ergebenden Verpflichtungen, insbesondere:

- **Meldung** an die zuständige Aufsichtsbehörde(n) innerhalb der gesetzlich vorgeschriebenen Frist,
- **Benachrichtigung** der betroffenen Personen, sofern diese gesetzlich erforderlich ist,

- **Ermittlung und Dokumentation** des Vorfalls (z. B. Art, Umfang, Ursache, Folgen der Datenpanne) sowie der ergriffenen Abhilfemaßnahmen.7.5 **Verzeichnisse von Verarbeitungstätigkeiten**
  Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO), in dem alle im Auftrag durchgeführten Verarbeitungsvorgänge aufgeführt werden. Dieses Verzeichnis wird dem Verantwortlichen auf Anfrage zur Verfügung gestellt, damit dieser seiner Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nachkommen kann.

7.6 **Datensicherheit und TOM**
Der Auftragsverarbeiter setzt die in Kapitel **4. Technische und organisatorische Maßnahmen (TOM)** beschriebenen Sicherheitsvorkehrungen zum Schutz der verarbeiteten personenbezogenen Daten um und überprüft deren Wirksamkeit regelmäßig. Änderungen an den TOM werden dem Verantwortlichen schriftlich oder elektronisch mitgeteilt.

7.7 **Mitarbeiterkontrolle und -verpflichtung**
Der Auftragsverarbeiter stellt sicher, dass alle Personen, die Zugang zu personenbezogenen Daten haben, mit den relevanten Datenschutz- und Datensicherheitsvorschriften vertraut sind und sich an die Vertragsvereinbarungen halten. Hierzu führt er Stichproben durch, um die Einhaltung der Verpflichtungen durch das Personal zu überprüfen.

7.8 **Nachweispflichten**
Der Auftragsverarbeiter führt geeignete Nachweise über die Erfüllung seiner datenschutzrechtlichen Pflichten und stellt diese dem Verantwortlichen auf Anfrage zur Verfügung. Dazu gehören insbesondere:

- Protokolle über Datensicherheits- und Datenschutzmaßnahmen,
- Beschreibungen von Schulungsmaßnahme sowie
- Nachweise zur Weisungsumsetzung

7.9 **Benennung eines Datenschutzbeauftragten**
Soweit gesetzlich vorgeschrieben (z. B. Art. 37 DSGVO, § 38 BDSG), benennt der Auftragsverarbeiter einen Datenschutzbeauftragten oder eine vergleichbare Ansprechperson, die für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich ist. Die Kontaktdaten sind dem Verantwortlichen schriftlich oder elektronisch mitzuteilen. Sollte keine Pflicht zur Benennung bestehen, ist der Auftragsverarbeiter dennoch angehalten, eine interne Stelle für Datenschutzbelange zu unterhalten oder zu benennen.

8. Übermittlung in Drittländer

8.1 **Grundsätze für Datentransfers in Drittländer**
Eine Übermittlung personenbezogener Daten in Drittländer (Staaten außerhalb der Europäischen Union [EU] bzw. des Europäischen Wirtschaftsraums [EWR]) oder an internationale Organisationen erfolgt nur, sofern folgende Voraussetzungen erfüllt sind:

- Vorlage von Standardvertragsklauseln, Angemessenheitsbeschlüssen oder genehmigten Verhaltensregeln.
- Vorherige Information des Verantwortlichen über Art und Umfang solcher Übermittlungen,
- Einhaltung der Grundsätze der DSGVO sowie ggf. weiterer anwendbarer nationaler und internationaler Datenschutzbestimmungen.

8.2 **Angemessenheitsbeschlüsse und geeignete Garantien**
Der Auftragsverarbeiter prüft, ob für das betreffende Drittland ein Angemessenheitsbeschluss der EU-Kommission vorliegt. Ist dies nicht der Fall, werden geeignete Garantien gemäß Art. 46 DSGVO eingesetzt, insbesondere:

- Standardvertragsklauseln (SCC) in der jeweils gültigen Fassung,
- Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules), falls vorhanden,
- Andere geeignete Garantien in Übereinstimmung mit den Anforderungen der DSGVO.

8.3 **Zusätzliche Schutzmaßnahmen**
Sofern sich aus einer Länder- oder Risikoanalyse ergibt, dass das Datenschutzniveau im Drittland nicht dem Standard der EU entspricht, verpflichtet sich der Auftragsverarbeiter in Abstimmung mit dem Verantwortlichen zu folgenden zusätzlichen Maßnahmen:

- **Technische Maßnahmen:** z. B. starke Verschlüsselung oder Pseudoanonymisierung vor der Übermittlung,
- **Organisatorische Maßnahmen:** z. B. klar geregelte Verfahren zur Konfliktbewältigung (z. B. behördliche Datenanfragen),
- **Vertragliche Ergänzungen:** z. B. Revisionsklauseln für die Standardvertragsklauseln, um auf Änderungen in der Rechtslage schnell reagieren zu können.

8.4 **Mitteilungspflichten**
Der Auftragsverarbeiter informiert den Verantwortlichen zeitnah, sofern er beabsichtigt, Daten in ein Drittland oder an eine internationale Organisation zu übertragen, sofern dies nicht bereits in diesem Vertrag ausdrücklich geregelt ist. Dabei teilt der Auftragsverarbeiter insbesondere folgende Informationen mit:

- **Zweck** der Übermittlung und **Kategorien** der betroffenen Daten,

- **Identität** des Empfängers (z. B. Subprozessor, Tochtergesellschaft, Kooperationspartner),
- **Geplante Rechtsgrundlage** (Angemessenheitsbeschluss, Standardvertragsklauseln etc.),
- **Besondere Risiken** oder Maßnahmen, die im jeweiligen Drittland zu beachten bzw. zu ergreifen sind.

8.5 **Dokumentation der Drittlandtransfers**
Der Auftragsverarbeiter dokumentiert sämtliche Übermittlungen in Drittländer in seinem Verzeichnis der Verarbeitungstätigkeiten oder in einem gesonderten Nachweis. Hieraus muss ersichtlich sein:

- **Grundlage** der Übermittlung (z. B. SCC, Angemessenheitsbeschluss),
- **Datum, Umfang und Zweck** der Übermittlung,
- **Empfänger** und Land, in das die Daten übermittelt werden.

8.6 **Rechtsansprüche und Gerichtsstand**
Die Vertragspartner werden im Falle von **Streitigkeiten oder Verfahren** im Zusammenhang mit grenzüberschreitenden Datenverarbeitungen unter Einbezug der zuständigen Datenschutzaufsichtsbehörden zusammenarbeiten. Sollten sich aus dem Drittlandtransfer rechtliche Risiken (z. B. aufgrund von Zugriffsbefugnissen staatlicher Stellen) ergeben, wird der Auftragsverarbeiter den Verantwortlichen umgehend informieren und alle möglichen Abwägungs- und Schutzmaßnahmen darlegen, um eine rechtskonforme Verarbeitung sicherzustellen.

9. Haftung und Schadensersatz

9.1 **Grundsätze**
Die Parteien haften einander für Schäden, die aus einer Verletzung ihrer vertraglichen oder gesetzlichen Pflichten im Zusammenhang mit dieser Auftragsverarbeitung entstehen, nach Maßgabe der einschlägigen datenschutzrechtlichen Vorschriften (insbesondere Art. 82 DSGVO) und den nachfolgenden Bestimmungen dieses Vertrags.

9.2 **Haftung des Auftragsverarbeiters**
Der Auftragsverarbeiter haftet für schuldhaft verursachte Schäden, sofern diese auf eine schuldhafte Verletzung seiner ihm obliegenden datenschutzrechtlichen Pflichten oder Weisungen des Verantwortlichen zurückzuführen sind. Dies gilt insbesondere für:

- **Verstöße gegen die Verpflichtungen aus diesem Vertrag**,
- **Nichteinhaltung gesetzlicher Vorgaben** (z. B. DSGVO, BDSG),
- **Nichtbeachtung** von Weisungen des Verantwortlichen.

Die Haftung umfasst alle Schäden, die unmittelbar oder mittelbar aus einem solchen Verstoß entstehen, einschließlich möglicher konkreter Schadenspositionen (z. b. Regressansprüche dritter, Bussgelder, Schmerzensgeldzahlunge), soweit diese gesetzlich oder vertraglich zuzurechnen sind.

9.3 **Haftung des Verantwortlichen**
Der Verantwortliche haftet gegenüber dem Auftragsverarbeiter für Schäden, die auf eine **schuldhafte Verletzung** seiner Pflichten zurückzuführen sind, insbesondere wenn:

- **Weisungen** erteilt wurden, die gegen geltendes Datenschutzrecht verstoßen, und der Auftragsverarbeiter den Verantwortlichen zuvor schriftlich oder elektronisch darauf hingewiesen hat,
- er es versäumt, den Auftragsverarbeiter rechtzeitig über zwingende Änderungen oder datenschutzrechtliche Anforderungen zu informieren, sodass dieser seinen Pflichten nicht ordnungsgemäß nachkommen konnte.

9.4 **Begrenzung der Haftung**

- **Ausschluss der Haftung für einfache Fahrlässigkeit:** Soweit gesetzlich zulässig, haften beide Parteien nur für Schäden, die durch **grobe Fahrlässigkeit** oder **Vorsatz** entstanden sind. Eine

darüberhinausgehende Haftung besteht nur bei Verletzung **wesentlicher Vertragspflichten** (Kardinalpflichten).
- **Haftungshöchstsumme:** Die Parteien können im Hauptvertrag oder in dieser Vereinbarung eine vereinbarte oder vorzusehende Haftungsgrenze (z. B. pauschaler Höchstbetrag, pro Ereignis oder pro Vertragslaufzeit) festlegen, sofern diese gesetzlich zulässig ist.
- **Haftung für Personenschäden** bleibt von den vorstehenden Regelungen unberührt und besteht im Rahmen der gesetzlichen Bestimmungen.

9.5 **Mitwirkungspflichten und Schadensminderung**
Um Schäden möglichst gering zu halten, verpflichten sich beide Parteien, einander bei der Rechtsverteidigung gegenüber Dritten oder im Falle von **Behördenverfahren** umfassend zu unterstützen und Informationen auszutauschen. Dies umfasst unter anderem:

- **Sofortige Information** über bekannte oder vermutete Datenschutzverstöße,
- Gemeinsame **Erarbeitung von Maßnahmen** zur Schadensbegrenzung oder -beseitigung,
- **Abstimmung** bei Verteidigungsstrategien gegenüber betroffenen Personen oder Aufsichtsbehörden.

9.6 **Freistellung**
Soweit Dritte (einschließlich betroffener Personen) gegen eine Partei Ansprüche aus vermeintlichen Datenschutzverstößen erheben, die nachweislich auf die Verantwortlichkeit oder Kausalität der jeweils anderen Partei zurückzuführen sind, stellt die verantwortliche Partei die in Anspruch genommene Partei im gesetzlich zulässigen Umfang von solchen Ansprüchen frei. Dies umfasst insbesondere Kosten für Rechtsberatung, Verteidigung und etwaige Schadensersatzzahlungen, sofern die verantwortliche Partei den Verstoß verursacht hat.

9.7 **Regress im Innenverhältnis**
Sofern eine Behörde, ein Gericht oder eine sonstige dritte Stelle eine der Parteien in Anspruch nimmt und diese Partei nachweislich aufgrund eines Verschuldens oder Mitverschuldens der anderen Partei in Anspruch genommen wurde, kann Reklamation, Rückgriff (Regress) geltend gemacht werden. Die Höhe der Regressforderung richtet sich nach der jeweiligen Verschuldensquote und ist unter Berücksichtigung der gesetzlichen Bestimmungen zu bemessen.

9.8 **Fortbestand der Haftungsregelungen**
Die Regelungen dieses Kapitels **Haftung und Schadensersatz** bleiben über das Ende dieser Vereinbarung hinaus gültig, soweit dies zur **Geltendmachung, Durchsetzung oder Abwehr** von Ansprüchen erforderlich ist, die sich aus diesem Vertrag ergeben oder damit in Zusammenhang stehen.

10. Beendigung und Rückgabe/Löschung

10.1 **Beendigung des Vertrags**
Die Vereinbarung tritt mit ihrer Unterzeichnung in Kraft und gilt für die Dauer des Hauptvertrags oder bis zu dessen Kündigung. Eine vorzeitige Beendigung aus wichtigem Grund, insbesondere bei schweren Datenschutzverstößen, bleibt unberührt.

10.2 **Verfahren bei Vertragsende**
Nach Beendigung dieser Vereinbarung oder auf Verlangen des Verantwortlichen vor Vertragsende ist der Auftragsverarbeiter verpflichtet, alle in seinem Besitz befindlichen personenbezogenen Daten, die im Rahmen der Auftragsverarbeitung verarbeitet wurden, nach Wahl des Verantwortlichen

- **entweder** vollständig und unwiderruflich zu löschen,
- **oder** dem Verantwortlichen in elektronischer Form zurückzugeben.

Hierbei sind auch sämtliche vorhandenen Kopien, Backups oder Replikationen zu berücksichtigen, sofern deren Aufbewahrung nicht aufgrund gesetzlicher Vorgaben (z. B. handels- oder steuerrechtliche Aufbewahrungsfristen) zwingend erforderlich ist.

10.3 **Dokumentation der Löschung oder Rückgabe**
Der Auftragsverarbeiter dokumentiert die Löschung oder Rückgabe aller personenbezogenen Daten und legt dem Verantwortlichen auf Verlangen schriftlich oder elektronisch einen Nachweis über die Durchführung vor. Dieser Nachweis muss in nachvollziehbarer Weise belegen,

- **welche Daten** wann und wie gelöscht oder zurückgegeben wurden,
- **welche Maßnahmen** ergriffen wurden, um eine unbefugte Wiederherstellung oder Offenlegung zu verhindern,
- **ob** gesetzliche Aufbewahrungsfristen oder andere zwingende Vorgaben die (Teil-)Aufbewahrung einzelner Daten erforderlich machten.

10.4 **Retention aufgrund gesetzlicher Pflichten**
Sofern gesetzliche Aufbewahrungsfristen oder andere zwingende rechtliche Anforderungen dem Löschen oder der Rückgabe entgegenstehen, werden die betreffenden personenbezogenen Daten nicht gelöscht, sondern in einer Form gesperrt, die eine weitere Verarbeitung ausschließt. Während dieser Zeit trägt der Auftragsverarbeiter dafür Sorge, dass die Daten weiterhin den Vorgaben dieses Vertrags und der geltenden Datenschutzvorschriften entsprechend geschützt sind.

10.5 **Weitergeltung der Vertraulichkeitsverpflichtungen**
Die in diesem Vertrag geregelten Verpflichtungen zur **Vertraulichkeit**, zum **Datenschutz** und zur **Beachtung von Weisungen** gelten über das Vertragsende hinaus fort, soweit dies zur Wahrung der Rechte und Freiheiten der betroffenen Personen sowie zum Schutz des Verantwortlichen erforderlich ist.

10.6 **Überprüfung und Übergangsregelungen**
Bei Einleitung der Vertragsbeendigung stimmen sich beide Parteien bezüglich der konkreten Schritte zur Rückgabe oder Löschung ab und definieren einen Übergabefahrplan oder Checkliste, um die sichere und geordnete Abwicklung aller Datenverarbeitungen zu gewährleisten. Bei strittigen Punkten oder Unsicherheiten kann der Verantwortliche externe Stellen z.B. die Aufsichtsbehörde oder Rechtsberater konsultieren, sofern dies für eine rechtssichere Vertragsbeendigung erforderlich ist.

11. Überwachung und Audits

11.1 **Recht des Verantwortlichen auf Überprüfung**
Der Verantwortliche oder ein von ihm beauftragter Dritter (z. B. externer Auditor) ist berechtigt, beim Auftragsverarbeiter Kontrollen durchzuführen, um sich von der Einhaltung der Regelungen dieser Vereinbarung, der DSGVO sowie weiterer einschlägiger Datenschutzvorschriften zu überzeugen. Dies schließt insbesondere Prüfungen vor Ort, Dokumentenprüfungen oder Systemtests ein.

11.2 **Ankündigung und Durchführung**

- **Ankündigungsfrist:** Der Verantwortliche teilt den geplanten Zeitpunkt der Audits sowie Umfang zehn Werktage im Voraus mit, damit sich der Auftragsverarbeiter bestmöglich darauf vorbereiten kann.
- **Kooperation und Unterstützung:** Der Auftragsverarbeiter unterstützt den Verantwortlichen in zumutbarem Umfang bei der Durchführung des Audits, stellterforderliche Unterlagen bereit und gewährt Zugang zu den relevanten Räumlichkeiten und Systemen.

11.3 **Kostenregelung**
Sofern nicht anders vereinbart, trägt jede Partei die eigenen Aufwendungen (z. B. Personal- und Reisekosten) für die Durchführung des Audits selbst. Sollten durch ein Audit beim Auftragsverarbeiter erhebliche Mehrkosten entstehen, kann der Auftragsverarbeiter mit dem Verantwortlichen eine Kostenberechnung oder Aufwandspauschale vereinbaren, sofern das Audit über das vereinbarte und zumutbare Maß hinaus geht..

11.4 **Vertraulichkeit**
Alle durch den Verantwortlichen oder einen von ihm beauftragten Dritten im Rahmen eines Audits gewonnenen Informationen sind vertraulich zu behandeln und dürfen nur für die Bewertung der Einhaltung dieser Vereinbarung und der datenschutzrechtlichen Pflichten verwendet werden. Die Informationen dürfen nicht an Dritte weitergegeben werden, es sei denn, gesetzliche Vorschriften oder behördliche Anordnungen erfordern dies.

11.5 **Einschränkungen**
Zur Wahrung der berechtigten Interessen des Auftragsverarbeiters oder Dritter kann der Auftragsverarbeiter den Zugang zu besonders sensiblen Bereichen oder Daten einschränken, sofern er dadurch keine wesentliche Überprüfung der Datenverarbeitung verhindert. Der Auftragsverarbeiter hat in solchen Fällen geeignete Alternativen (z. b. Bereitstellung anonymisierter Berichte) aufzuzeigen, um dennoch eine hinreichende Prüfung zu ermöglichen.

11.6 **Regelmäßige Überprüfung und Zertifizierungen**
Der Auftragsverarbeiter bemüht sich, regelmäßig geeignete Compliance- oder Sicherheits-Zertifizierungen (z. B. ISO 27001, TISAX) durchzuführen oder zu erneuern. Auf Verlangen stellt der Auftragsverarbeiter dem Verantwortlichen aktuelle Zertifizierungsnachweise, Prüfberichte oder Management-Summaries zur Verfügung, sodass dieser sich ein Bild vom Datenschutzniveau und der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen machen kann.

11.7 **Dokumentation der Ergebnisse**
Die Ergebnisse der Audits oder sonstiger Prüfungen werden vom Verantwortlichen oder dessen Beauftragten dokumentiert. Der Auftragsverarbeiter kann auf Einwilligung oder Gegenzeichnung bestehen, wenn Beanstandungen oder Mängel festgestellt werden und entsprechende Umsetzungsschritte und Fristen vereinbart werden sollen. In Streitfällen können sich die Parteien zur Klärung an geeignete Stellen wenden.

12. Sonstige Regelungen

12.1 **Vertraulichkeit**
Die Parteien verpflichten sich, sämtliche im Rahmen dieses Vertrags sowie des zugrundeliegenden Hauptvertrags erlangten Informationen, Daten und Geschäftsgeheimnisse des jeweils anderen Vertragspartners vertraulich behandeln. Diese Verpflichtung gilt auch über das Ende des Vertragsverhältnisses hinaus, sofern und solange keine anderweitigen gesetzlichen oder vertraglichen Bestimmungen entgegenstehen.

- **Ausnahmen:** Gesetzliche Offenlegungspflichten oder behördliche Anordnungen können die Partei zur Herausgabe von Informationen verpflichten. In diesem Fall ist der betroffene Vertragspartner schriftlich oder elektronisch zu unterrichten.

12.2 **Gerichtsstand und anwendbares Recht**

- **Gerichtsstand:** Sofern rechtlich zulässig, vereinbaren die Parteien als ausschließlichen Gerichtsstand Köln.
- Anwendbares Recht: Es gilt ausschließlich deutsches Recht unter Ausschluss des UN-Kaufrechts und anderer kollisionsrechtlicher Vorschriften, sofern nicht zwingende Bestimmungen eines anderen Rechtsraums einschlägig sind.

Siteware GmbH, Andreas Jansen

ANLAGE 1: Verzeichnis der Verarbeitungstätigkeiten

Allgemeine Angaben

Name des Auftragsverarbeiters: Siteware GmbH
Adresse des Auftragsverarbeiters: Am Weilsberg 11, 51789 Lindlar, Deutschland

---

Verarbeitungstätigkeiten

1. Bereitstellung von SaaS-Diensten (z. B. KI-Werkzeuge, Chatbots, Conversational AI)

- **Zweck der Verarbeitung:** Unterstützung bei alltäglichen Aufgaben wie Kommunikation, Textgenerierung, Datenanalyse und Protokollierung.
- **Rechtsgrundlage:** Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b DSGVO.
- **Kategorien betroffener Personen:** Kunden, Mitarbeiter:innen, Lieferanten.
- **Kategorien personenbezogener Daten:** Kontaktdaten, Inhaltsdaten, Protokolldaten, Nutzungsdaten.
- **Empfänger der Daten:** Keine Übermittlung an Dritte ohne vorherige Genehmigung, Subprozessoren gemäß Anlage Unterauftragsverarbeiter.
- **Drittlandübermittlungen:** Möglich gemäß Standardvertragsklauseln oder Angemessenheitsbeschlüssen.
- **Löschfrist:** Daten werden gemäß Vertrag oder gesetzlicher Aufbewahrungsfristen gelöscht.

2. Datenanalyse und automatisierte Texterstellung

- **Zweck der Verarbeitung:** Generierung von Berichten, Analysen und Textinhalten auf Basis von Kundendaten.
- **Rechtsgrundlage:** Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO oder Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b DSGVO.
- **Kategorien betroffener Personen:** Kunden, Mitarbeitende, Interessenten.
- **Kategorien personenbezogener Daten:** Eingabedaten, Analyseergebnisse, Protokolldaten.
- **Empfänger der Daten:** Interne Verarbeitung durch Siteware, Subprozessoren nur mit Zustimmung.
- **Drittlandübermittlungen:** Nur bei Vorliegen geeigneter Garantien.
- **Löschfrist:** Daten werden anonymisiert, sobald der Zweck erfüllt ist, oder nach Kundenanweisung gelöscht.

3. Kunden- und Nutzerkommunikation

- **Zweck der Verarbeitung:** Kontaktaufnahme, Support, Benachrichtigungen.
- **Rechtsgrundlage:** Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b DSGVO.
- **Kategorien betroffener Personen:** Kunden, potenzielle Neukunden, Mitarbeitende.
- **Kategorien personenbezogener Daten:** Name, E-Mail-Adresse, Kommunikationsinhalte.

- **Empfänger der Daten:** Verarbeitung innerhalb von Siteware, Weitergabe an Support-Tools/Subprozessoren bei Bedarf.
- **Drittlandübermittlungen:** Verarbeitung in Drittländern mit SCC oder Angemessenheitsbeschluss.
- **Löschfrist:** Nach Abschluss der Kommunikation und Ablauf der gesetzlichen Aufbewahrungsfristen.

4. Datenmanagement und Hosting

- **Zweck der Verarbeitung:** Speicherung und Verwaltung von Kundendaten, Betrieb der Plattform.
- **Rechtsgrundlage:** Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b DSGVO.
- **Kategorien betroffener Personen:** Kunden, Mitarbeitende.
- **Kategorien personenbezogener Daten:** Nutzungsdaten, Log-Daten, Systemdaten.
- **Empfänger der Daten:** Hosting-Anbieter gemäß Anlage Unterauftragsverarbeiter.
- **Drittlandübermittlungen:** Verarbeitung in zertifizierten Rechenzentren mit SCC.
- **Löschfrist:** Nach Vertragsbeendigung oder nach Kundenanweisung.

5. Support und Fehleranalyse

- **Zweck der Verarbeitung:** Fehlerbehebung, Systemdiagnose, Kundenanfragen.
- **Rechtsgrundlage:** Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b DSGVO.
- **Kategorien betroffener Personen:** Kunden, interne Mitarbeitende.
- **Kategorien personenbezogener Daten:** Protokolldaten, Fehlerberichte, Nutzungsdaten.
- **Empfänger der Daten:** Technischer Support, autorisierte Subprozessoren.
- **Drittlandübermittlungen:** Möglich gemäß dokumentierten Garantien (z. B. SCC).
- **Löschfrist:** Nach Abschluss der Fehlerbehebung oder Ablauf der Aufbewahrungsfrist.

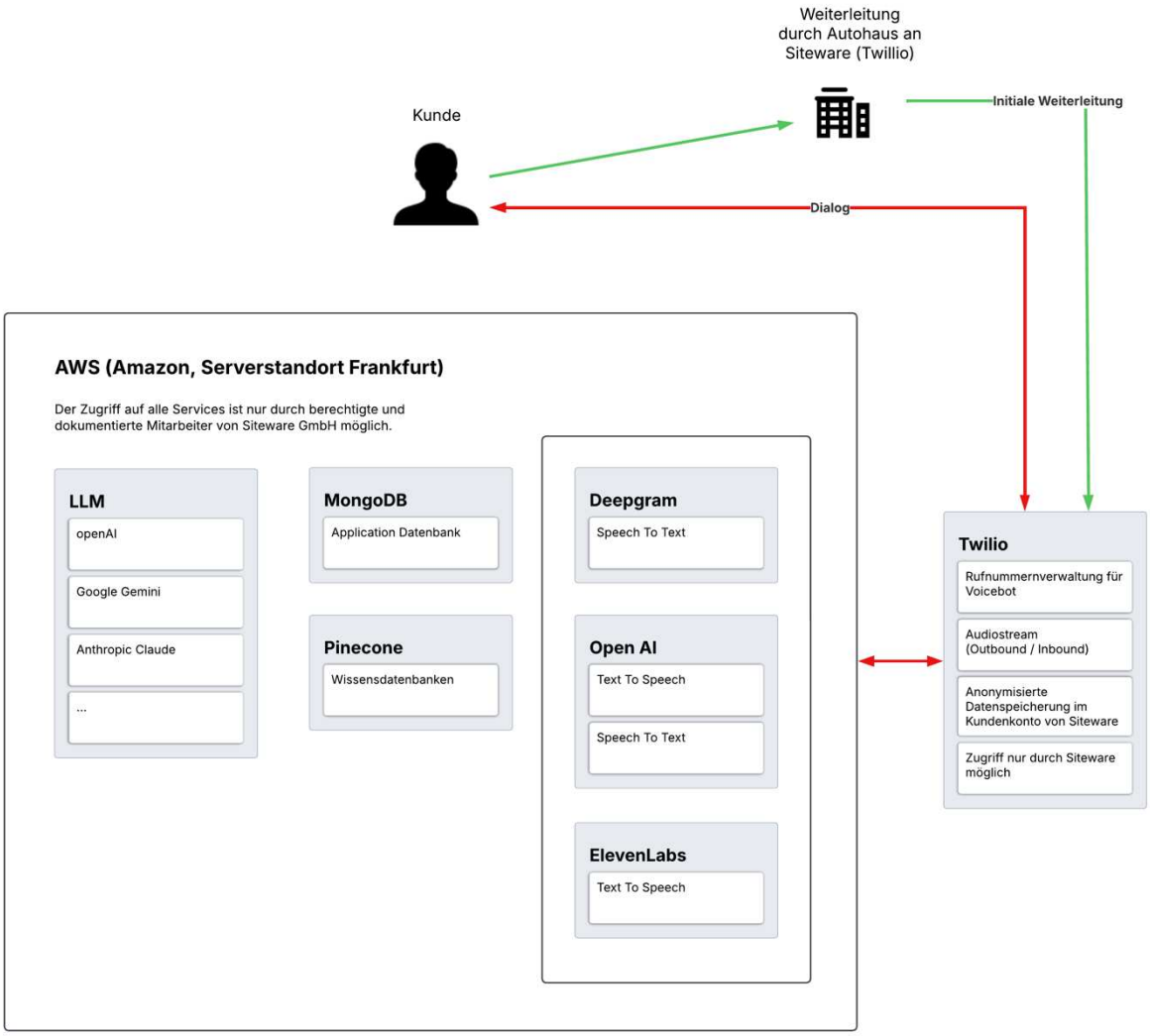
Allgemeine Schutzmaßnahmen

- **Technische Maßnahmen:** Verschlüsselung, Zugriffskontrollen, Pseudonymisierung.
- **Organisatorische Maßnahmen:** Schulungen, Vertraulichkeitsvereinbarungen, regelmäßige Audits.

Anlage 2: Subunternehmen von Siteware GmbH

Partner-Name	Adresse	Land	Garantielseitungen	Relevanz der Vereinbarung für folgende Bereiche
Atlassian Pty Ltd	Level 6, 341 George Street, Sydney NSW 2000, Australien	Australien	Standardvertragsklauseln	Sicherer Zugriff auf Tools (z. B. Jira, Confluence), regelmäßige Schwachstellenscans, Auditberichte
Amazon Web Services, Inc. (AV	410 Terry Avenue North, Seattle, WA 98109, USA	USA	Standardvertragsklauseln	Identity Access Management (IAM), Firewalls und Sicherheitsgruppen, regelmäßige Penetrationstests, Cloud-native Sicherheitsservices (z. B. IAM, VPC), kontinuierliche Überprüfung der Sicherheitskonfigurationen
Borlabs GmbH	Georg-Wilhelm-Straße 17, 21107 Hamburg, Deutschland	Deutschland	Nicht erforderlich (innerhalb der EI	DSGVO-konforme Datenverarbeitung, Verschlüsselung und Backups, rollenbasierte Zugangskontrolle
Deepgram	148 Townsend Street, San Francisco, CA 94107, USA	USA	Standardvertragsklauseln	Speicherung von Audiodaten in pseudonymisierter Form, regelmäßige Penetrationstests, Schutz vor Datenabfluss
ElevenLabs	2140 S Dupont Hwy, Camden, DE 19934, USA	USA	Standardvertragsklauseln	Datenverschlüsselung (AES-256), Multi-Faktor-Authentifizierung (MFA), Sicherheitsprotokolle (TLS/SSL), Zugriffskontrollsysteme
FastBill GmbH	Theodor-Heuss-Allee 112, 60486 Frankfurt am Main, Deutschland	Deutschland	Nicht erforderlich (innerhalb der EI	Sichere Finanzdatenverarbeitung, regelmäßige Sicherheitsüberprüfungen, revisionssichere Speicherung von Transaktionsdaten
GitHub Inc.	88 Colin P Kelly Jr Street, San Francisco, CA 94107, USA	USA	Teilnahme am EU-U.S.	Verschlüsselung bei der Datenübertragung, Zugriffsbeschränkungen auf Repositories, Sicherheitsanalysen von Code
Google Inc.	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	USA	Standardvertragsklauseln	ISO 27001-Zertifizierung, Verschlüsselung im Ruhezustand und bei Übertragung, Kontrollsysteme für globale Datenzentren
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	Irland	Nicht erforderlich (innerhalb der EI	Datenlokalisierung und Schutzmaßnahmen in globalen Datenzentren, strenge Zugriffskontrollen
Mittwald Hosting	Königsberger Straße 4-6, 32339 Espelkamp, Deutschland	Deutschland	Nicht erforderlich (innerhalb der EI	Zugriffsbeschränkungen auf Serverräume, DSGVO-konforme Datenverarbeitung, Protokollierung von Änderungen
MongoDB	1633 Broadway, 38th Floor, New York, NY 10019, USA	USA	Standardvertragsklauseln	Zugriffskontrollen auf Datenbanken, Verschlüsselung auf Datenebene, Auditing-Funktionalität
OpenAI	3180 18th Street, San Francisco, CA 94110, USA	USA	Standardvertragsklauseln	Pseudonymisierung, End-to-End-Verschlüsselung, Protokollierung von Datenzugriffen, Notfallpläne für Datenpannen
Pinecone	228 Park Avenue S, PMB 40577, New York, NY 10003, USA	USA	Standardvertragsklauseln	Verschlüsselung der Datenkommunikation, automatisches Backup, Protokollierung von API-Zugriffen
Stripe Payment	354 Oyster Point Boulevard, South San Francisco, CA 94080, USA	USA	Standardvertragsklauseln	PCI-DSS-Zertifizierung, Tokenisierung von Zahlungsdaten, Zugriffsbeschränkungen auf sensitive Finanzdaten
Twilio Inc.	375 Beale Street, Suite 300, San Francisco, CA 94105, USA	USA	Standardvertragsklauseln	Authentifizierung für alle API-Zugriffe, Verschlüsselung bei der Übertragung, Überwachung und Protokollierung
Zoom Communications Inc.	55 Almaden Boulevard, 6th Floor, San Jose, CA 95113, USA	USA	Standardvertragsklauseln	End-to-End-Verschlüsselung für Meetings, kontrollierter Zugriff auf Aufzeichnungen, regelmäßige Sicherheitsupdates

DATENSTRÖME SITEWARE VOICEBOT



Beim Einsatz des Telefonbots im Autohaus sind mehrere Systeme und Dienstleister beteiligt. Die Kommunikation erfolgt über Twilio und AWS, und es werden personenbezogene Daten verarbeitet. Im Folgenden werden die Datenströme und die datenschutzrelevanten Aspekte beschrieben:

1. **Anrufannahme und Weiterleitung (Twilio)**
    - **Datenfluss:** Der Kunde ruft die Service-Nummer des Autohauses an. Der Anruf wird direkt zu einer Twilio-Nummer weitergeleitet.
    - **Verarbeitete Daten:** Telefonnummer des Anrufers, Zeitstempel, Verbindungsdauer.
    - **Datenschutzaspekte:** Twilio speichert Verbindungsdaten zur Abrechnung und Fehleranalyse im Siteware-Account.
2. **Sprachdatenübertragung an AWS**
    - **Datenfluss:** Twilio leitet die Sprachdaten in Echtzeit an den Server von Sitware bei Amazon Web Services (AWS, Standort Frankfurt) weiter.
    - **Verarbeitete Daten:** Sprachaufnahmen, die potenziell personenbezogene Daten enthalten (z. B. Name, Kfz-Kennzeichen, Terminwünsche).
    - **Datenschutzaspekte:** Die Übertragung erfolgt Ende-zu-Ende verschlüsselt.
3. **Verarbeitung durch den Telefonbot (OpenAI)**
    - **Datenfluss:** Die Sprachdaten werden durch AWS an die OpenAI-Schnittstelle weitergeleitet, wo sie in Text umgewandelt und analysiert werden. Die Antworten des Bots werden wiederum in Sprache umgewandelt und zurückgesendet.
    - **Verarbeitete Daten:** Transkribierter Text der Sprachaufnahmen, generierte Antworten.
    - **Datenschutzaspekte:** Die Nutzung der OpenAI-API erfolgt über eine sichere Verbindung. Die Daten werden nicht zur Verbesserung des Modells genutzt.

4. **Rückleitung an den Anrufer (Twilio)**
    - **Datenfluss:** Die vom Bot generierte Sprachausgabe wird über AWS an Twilio zurückgeleitet und von dort an den Anrufer übertragen.
    - **Verarbeitete Daten:** Generierte Sprachantworten, Verbindungsmetadaten.
    - **Datenschutzaspekte:** Die Übertragung erfolgt verschlüsselt.

Implementierte Datenschutzmaßnahmen:

- **Datenminimierung:** Nur die für die Serviceabwicklung notwendigen Daten werden gespeichert.
- **Zugriffs- und Berechtigungskonzept:** Nur autorisierte Personen dürfen auf die verarbeiteten Daten zugreifen.
- **Regelmäßige Sicherheitsprüfungen:** Verschlüsselung, Sicherheitsupdates und Monitoring der Systeme

Anlage TOM

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO
zum Auftragsverarbeitungsvertrag (AVV) der Siteware GmbH
Stand: 03 / 2026

Die nachfolgenden technischen und organisatorischen Maßnahmen (TOM) beschreiben die Sicherheitsvorkehrungen, die die Siteware GmbH als Auftragsverarbeiter gemäß Art. 32 DSGVO zum Schutz personenbezogener Daten implementiert hat. Diese Anlage ist Bestandteil des zwischen den Parteien geschlossenen Auftragsverarbeitungsvertrags (AVV) und konkretisiert die in Kapitel 4 des AVV beschriebenen Maßnahmen.

---

1. Vertraulichkeit

M.1.1 Zutrittskontrolle

- **1) Schließanlage** Einsatz einer Schließanlage
- **2) Schlüsselverwaltung** Schlüsselregelung mit Dokumentation der Schlüssel (z. B. Schlüsselbuch)

M.1.2 Zugangskontrolle

- **1) Authentifikation mit Benutzer + Passwort** Authentifikation mit Benutzer + Passwort
- **2) Benutzerberechtigungen** Benutzerberechtigungen verwalten (z. B. bei Eintritt, Änderung, Austritt)
- **3) Firewall** Einsatz von Firewalls zum Schutz des Netzwerkes
- **4) Verschlüsselung von Datenträgern** Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

M.1.3 Zugriffskontrolle

- **1) Berechtigungskonzept** Rollenbasiertes Berechtigungskonzept
- **2) Passwortrichtlinien** Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
- **3) Sichere Aufbewahrung** Sichere Aufbewahrung von Datenträgern
- **4) Verschlüsselung von Datenträgern** Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

M.1.4 Weitergabekontrolle

- **1) E-Mail-Verschlüsselung** E-Mail-Verschlüsselung mit S/MIME oder PGP Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren)
- **2) SSL / TLS Verschlüsselung** Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet

M.1.5 Trennungsgebot

- **1) Physikalische Trennung der Daten** Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- **2) Produktiv- und Testsystem** Trennung von Produktiv- und Testsystem

M.1.6 Pseudonymisierung

- **1) Trennung Kontaktdaten** Trennung von Kontaktdaten und anderen Daten

- **2) Trennung Stammdaten** Trennung von Kundenstammdaten und Auftragsdaten

M.1.7 Verschlüsselung

- **1) Speicherung** Verschlüsselte Datenspeicherung (z. B. Dateiverschlüsselung nach AES256 Standard)
- **2) Übertragung** Verschlüsselte Datenübertragung (z. B. E-Mail-Verschlüsselung nach PGP oder S/MIME, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL)

---

2. Integrität

M.2.1 Eingabekontrolle

- **1) Personalisierte Benutzernamen** Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- **2) Protokollierung** Protokollierung der Eingabe, Änderung und Löschung von Daten
- **3) Zugriffsrechte** Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe

---

3. Verfügbarkeit und Belastbarkeit

M.3.1 Verfügbarkeitskontrolle

- **1) Antivirensoftware** Einsatz von Antivirensoftware zum Schutz vor Malware
- **2) Backup- und Recoverykonzept** Regelmäßige Datensicherung mit definierten Wiederherstellungsverfahren

M.3.2 Wiederherstellbarkeit

- **1) Verwendung einer Firewall** Einsatz einer Firewall zum Schutz der Infrastruktur
- **2) Spamfilter** Verwendung und regelmäßige Aktualisierung eines Spamfilters

---

4. Weitere Maßnahmen

M.4.1 Auftragskontrolle

- **1) Audits** Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
- **2) AV-Vertrag** Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO

M.4.2 Managementsystem

- **1) Audits** Durchführung regelmäßiger interner Audits
- **2) DSB** Benennung eines Datenschutzbeauftragten
- **3) Schulung** Schulungen aller zugriffsberechtigten Mitarbeiter; regelmäßig stattfindende Nachschulungen
- **4) Softwaregestützte Tools** Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (audatis MANAGER)
- **5) Verpflichtung** Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO

Die aufgeführten Maßnahmen werden regelmäßig auf ihre Wirksamkeit überprüft und bei Bedarf angepasst. Änderungen werden dem Verantwortlichen innerhalb einer Woche schriftlich oder elektronisch mitgeteilt (vgl. Kapitel 4.4 des AVV). Diese Anlage ist Bestandteil des Auftragsverarbeitungsvertrags zwischen dem Verantwortlichen und der Siteware GmbH, Am Weilsberg 11, 51789 Lindlar.