

Auftragsverarbeitungsvertrag

Anlage zu den Nutzungsbedingungen (AGB) für die ConnectWunder-Software, die der Auftraggeber spätestens beim ersten Login in das ConnectWunder-Backend bestätigt.

zwischen

demjenigen Nutzer bzw. derjenigen juristischen Person oder natürlichen Person als Unternehmer, der/die die ConnectWunder-Leistungen bezieht – nachfolgend „Auftraggeber“/„Verantwortlicher“ oder „Controller“.

im Folgenden Auftraggeber (AG) genannt

und

Yonju EOOD
ul.Brezovska 36 et.4
4003 Plovdiv
Bulgaria

im Folgenden Auftragsverarbeiter (AV) genannt

wird als Anlage zu dem oben bezeichneten Hauptvertrag nach Vorgabe der Datenschutzgrundverordnung zum Schutz der von dem Auftragsverarbeiter verarbeiteten Daten des Auftraggebers vereinbart:

§ 1 Vertragsinhalt und Laufzeit

- (1) Inhalt des Vertragsanhangs ist die Datenverarbeitung, die der Auftragsverarbeiter für den Auftraggeber im Rahmen des Hauptvertrages ausführt. Dies umfasst jede Verarbeitung von personenbezogenen Daten im Rahmen des Hauptvertrages gem. Art. 28 DSGVO.
- (2) Zweck der Verarbeitung ist die Erfüllung des Hauptvertrages durch den Auftragsverarbeiter und die Erfüllung der Verpflichtungen beider Parteien aus der DSGVO.
- (3) Die Laufzeit dieses Vertrages ergibt sich aus seinem Zweck. Er läuft für die Dauer des Hauptvertrages einschließlich der Erfüllung von Gewährleistungspflichten oder sonstigen nachvertraglichen Pflichten durch den Auftragsverarbeiter. Wird der Hauptvertrag gekündigt, bleibt dieser Vertrag für die Dauer der verbleibenden nachvertraglichen Pflichten bestehen und endet erst mit der Vollbeendigung des Hauptvertrages und der Löschung oder Rückgabe der Daten nach Maßgabe dieses Anhangs.
- (4) Die Verarbeitung kann im Rahmen der Nutzung der ConnectWunder-Software einschließlich gebuchter oder aktivierter Module, Schnittstellen und Funktionen erfolgen. Hierzu können insbesondere Funktionen zur Organisation von Geschäftsbeziehungen, Kommunikation, Meetings, Dokumenten, Arbeitsprozessen, künstlicher Intelligenz, Automatisierung und Schnittstellenanbindung gehören. Die Einzelheiten ergeben sich aus Anlage 1.

§ 2 Art der Daten, der Betroffenen und der Verarbeitung, Vertragsort

- (1) Dieser Vertragsanhang gilt für alle Arten von Verarbeitungen gem. Art. 4 Nr. 2 DSGVO.
- (2) Die Art der verarbeiteten Daten umfasst alle Daten, die der Auftragsverarbeiter für den Auftraggeber im Rahmen des Hauptvertrages verarbeitet. Die Daten sind in Anlage 1 zu diesem Vertrag näher aufgeführt.
- (3) Die Kategorien der von diesem Vertrag betroffenen Personen ergeben sich aus der Datennutzung durch den Auftraggeber, sie sind in Anlage 1 zu diesem Vertragsanhang näher aufgeführt.
- (4) Eine Verarbeitung außerhalb der europäischen Union ist nur in den gesetzlich erlaubten Fällen möglich.

§ 3 Verantwortung und Weisungen

- (1) Dieser Vertragsanhang ändert nichts daran, dass der Auftraggeber für die Einhaltung der Datenschutzgesetze und eine rechtmäßige Weitergabe der Daten an den Auftragsverarbeiter gem. Art. 4 Abs. 7 DSGVO allein Verantwortlicher bleibt. Dies gilt auch für alle Verarbeitungen,

die Gegenstand dieses Vertragsanhangs sind.

(2) Weisungen im Rahmen der Auftragsverarbeitung werden von dem Auftraggeber zum einen im Hauptauftrag festgelegt. Anschließend können sie mündlich oder in Textform erteilt werden. Der Auftragsverarbeiter hat einen Anspruch darauf, dass mündliche Weisungen unverzüglich auch in Textform bestätigt werden (z.B. E-Mail oder sonstige elektronische Form). Der Auftragsverarbeiter kann – außer bei Gefahr im Verzuge – die Ausführung der Weisung von einer vorherigen Weisung in Textform abhängig machen.

(3) Weisungen, die über den Inhalt des Hauptvertrages hinausgehen, sind für den Auftragsverarbeiter nur verbindlich, wenn sie nach dem Sinn des Hauptvertrages und auf Grund der Bestimmungen der DSGVO erforderlich sind (z.B. in einer Angriffssituation erforderliche Sicherungen). Sie sind gleichzeitig eine Zusatzleistung im Rahmen des Hauptvertrages und nach den dortigen Bestimmungen zusätzlich – ersatzweise anhand der ortsüblichen und angemessenen Vergütung – zu entrichten.

(4) Ist der Auftragsverarbeiter nicht zur Ausführung der Weisung verpflichtet, kann er die Ausführung verweigern, bis der Auftraggeber die Zusatzleistung bestätigt und kostenpflichtig beauftragt hat. Die Ausführung der Weisung ist kein Verzicht auf einen Anspruch auf zusätzliche Vergütung.

(5) Ist dem Auftragsverarbeiter die Ausführung einer Weisung nicht zuzumuten, etwa weil Ihre Befolgung technisch nicht möglich ist, kann der Auftragsverarbeiter den Hauptvertrag kündigen, sofern zwischen den Parteien keine andere Lösung gefunden wird. Ein Beispiel ist etwa eine Leistungserbringung durch den Auftragsverarbeiter auf einer technischen Plattform mit anderen Auftraggebern einer Auftragsverarbeitung, bei der die Weisung nicht ohne Konsequenzen für andere Vertragspartner des Auftragsverarbeiters befolgt werden kann (z.B. Daten können nicht getrennt werden).

(6) Erteilt der Auftraggeber eine rechtswidrige Weisung, hat er die daraus entstehenden Kosten zu tragen, einschließlich der Rechtsberatungs- oder -vertretungskosten des Auftragsverarbeiters.

(7) Weisungen des Auftraggebers können sich auch aus der Nutzung, Administration oder Konfiguration der ConnectWunder-Software ergeben, insbesondere durch Einstellungen innerhalb der Plattform, aktivierte Module, angebundene Schnittstellen, Support-Anfragen oder dokumentierte elektronische Anweisungen des Auftraggebers.

(8) Der Auftraggeber bleibt für die Rechtmäßigkeit seiner Weisungen verantwortlich. Der Auftragsverarbeiter ist nicht verpflichtet, Weisungen des Auftraggebers rechtlich zu prüfen. Erkennt der Auftragsverarbeiter jedoch einen offensichtlichen Verstoß gegen geltendes Datenschutzrecht oder sonstiges für ihn bindendes Recht, kann er die Ausführung der Weisung bis zur Klärung aussetzen.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, die Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers zu verarbeiten. Dies gilt nicht, soweit der Auftragsverarbeiter zu einer anderen Verarbeitung aufgrund eines in der europäischen Union für ihn gültigen Rechts verpflichtet ist. Der Auftragsverarbeiter kann eine Weisung, die gegen geltendes Recht verstößt, das auch für ihn bindend ist, zurückweisen und ist zu Ihrer Ausführung nicht verpflichtet. Der Auftragsverarbeiter wird in einem solchen Fall den Auftraggeber auffordern, eine rechtmäßige Weisung zu erteilen.

(2) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung von Rechtsansprüchen betroffener Personen aus den Artt. 12-23 DSGVO Betroffener im Rahmen seiner Kapazitäten. Er benennt dem Auftraggeber einen Ansprechpartner im Rahmen des Datenschutzes.

(3) Der Auftragsverarbeiter wird in seinem Bereich für den Auftraggeber die Pflichten aus Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen einhalten und in angemessenen Abständen überprüfen.

(4) Der Auftragsverarbeiter organisiert seinen Betrieb derart, dass er den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft gem. Art. 32 DSGVO unter Berücksichtigung seiner zumutbaren Möglichkeiten und Einrichtungen technische und organisatorische Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Die derzeitigen technischen und organisatorischen Maßnahmen sind in Anlage 2 zu diesem Vertrag festgehalten.

(5) Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere eingesetzte Dritte über die Anforderungen des Datenschutzes unterrichtet sind und entsprechend angeleitet, geschult und überwacht werden. Weiter gewährleistet der Auftragsverarbeiter, dass diese Personen verpflichtet sind, die

Daten nicht außerhalb der Weisungen des Auftraggebers zu verarbeiten und die Daten vertraulich zu behandeln sowie, dass diese Verschwiegenheitspflicht auch nach der Beendigung des Hauptvertrages fort gilt.

(6) Daten, die Gegenstand dieser Auftragsverarbeitung sind, berichtigt, sperrt oder löscht der Auftragsverarbeiter nur entsprechend dieses Vertrages oder nach Weisung des Auftraggebers. Derartige Weisungen des Auftraggebers sind auch nachvertraglich verbindlich.

(7) Der Auftragsverarbeiter unterrichtet den Auftraggeber, sofern er Kenntnis davon erlangt, dass Daten des Auftraggebers verletzt wurden oder werden. Er trifft zur Gefahrenabwehr eigenständig die erforderlichen Maßnahmen zur Datensicherung und mindert soweit möglich die Folgen für die Betroffenen. Er spricht sich so schnell wie möglich mit dem Auftraggeber ab.

(8) Nach Abschluss der Verarbeitungstätigkeit löscht der Auftragsverarbeiter nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück. Dies gilt nicht, soweit die Daten nach dem anwendbaren Recht weiter gespeichert bleiben müssen oder sich aus dem Vertrag ein anderes ergibt. Erteilt der Auftraggeber keine Weisung, gilt die Löschung als vereinbart.

(9) Soweit die ConnectWunder-Software Funktionen mit künstlicher Intelligenz, automatisierter Verarbeitung, Transkription, Zusammenfassung, Kommunikationsanalyse, Medienverarbeitung, Schnittstellenanbindung oder automatisierter Datenübertragung bereitstellt, erfolgt die Verarbeitung personenbezogener Daten ausschließlich im Rahmen der vom Auftraggeber gebuchten, aktivierten, angebundenen oder angewiesenen Funktionen. Eine Verarbeitung personenbezogener Daten des Auftraggebers zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

§ 5 Vergütung

(1) Für alle Leistungen nach diesem Vertrag hat der Auftragsverarbeiter Anspruch auf eine zusätzliche Vergütung nach Maßgabe des Hauptvertrages, ersatzweise der ortsüblichen und angemessenen Vergütung. Dies gilt nicht, soweit der Hauptvertrag ausdrücklich ein anderes regelt oder solche Ansprüche aufgrund Gewährleistung oder Verschulden des Auftragsverarbeiters ausgeschlossen sind.

(2) Die Verpflichtung zur Vergütung gilt bis zur Vollbeendigung dieses Anhangs und endet nicht mit dem Hauptvertrag.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber darf keine Weisung erteilen, die gegen geltendes Recht verstößt. Der Auftraggeber ist weiter Verantwortlicher für die Daten, es ist daher seine Sache, sich über die geltenden Gesetze zu informieren und sich dazu beraten zu lassen und dem Auftragsverarbeiter nur solche Weisungen zu erteilen, die rechtmäßig sind.

(2) Dies gilt insbesondere auch für personenbezogene Daten, die der Auftraggeber im Rahmen von Kommunikationsfunktionen, Meeting- oder Call-Verarbeitung, Messaging, Chat-Verarbeitung, Transkription, Medienverarbeitung, künstlicher Intelligenz, Automatisierungen, Schnittstellen, Writeback-Funktionen oder angebundenen Drittplattformen in die ConnectWunder-Software einbringt oder über diese verarbeiten lässt. Der Auftraggeber ist verantwortlich dafür, dass hierfür die erforderlichen Rechtsgrundlagen, Informationspflichten und – soweit erforderlich – Einwilligungen vorliegen.

(3) Der Auftraggeber ist insbesondere dafür verantwortlich, dass Teilnehmer von Meetings oder Calls, Kommunikationspartner, Empfänger von Nachrichten, Chat-Partner, Kunden, Interessenten, Mitarbeiter und sonstige betroffene Personen ordnungsgemäß informiert werden, soweit dies nach den anwendbaren Datenschutzgesetzen oder sonstigen gesetzlichen Vorschriften erforderlich ist.

(4) Der Auftraggeber ist verpflichtet, die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters zu erfragen und zu prüfen. Er trägt die Verantwortung dafür, dass die Maßnahmen des Auftragsverarbeiters für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau darstellen.

(5) Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich und vollständig, wenn ihm Tatsachen offenbar werden, dass bei der Datenverarbeitung Fehler oder Unregelmäßigkeiten vorkommen.

(6) Der Auftraggeber benennt auf Anforderung des Auftragsverarbeiters einen Ansprechpartner für alle Datenschutzfragen in seinem Hause.

(7) Der Auftraggeber ist verpflichtet, Forderungen von Betroffenen auf Berichtigung, Löschung, Sperrung oder Auskunft zu bearbeiten. Der Auftragsverarbeiter wird die betroffene Person an den Auftraggeber verweisen, sofern das aufgrund der Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person

vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 7 Nachweise

(1) Der Auftragsverarbeiter informiert den Auftraggeber über alle Maßnahmen zur Einhaltung der Anforderungen des Art. 28 DSGVO und ermöglicht in zumutbarem Rahmen Überprüfungen. § 5 gilt entsprechend.

(2) Der Auftragsverarbeiter ist berechtigt, von dem Auftraggeber und/oder dessen Prüfer eine Verschwiegenheitserklärung zu verlangen. Der Auftraggeber kann einen unabhängigen externen Prüfer benennen, sofern er dem Auftragsverarbeiter eine Kopie des Auditberichts zur Verfügung stellt. Wettbewerber des Auftragsverarbeiters oder Personen, die dem Auftragsverarbeiter sonst nicht zumutbar sind, kann der Auftragsverarbeiter ablehnen.

(3) Für Prüfungen einer Behörde gelten diese Regeln entsprechend, einschließlich § 5.

(4) Der Auftragsverarbeiter kann Nachweise vorrangig durch geeignete Dokumentation, Sicherheitsinformationen, Erklärungen, technische Beschreibungen oder Informationen zu eingesetzten Unterauftragsverarbeitern erbringen, soweit hierdurch ein angemessener Nachweis der Einhaltung der Pflichten aus diesem Vertrag möglich ist. Eine Vor-Ort-Prüfung ist nur erforderlich, soweit ein gleichwertiger Nachweis nicht auf andere zumutbare Weise erbracht werden kann.

§ 8 Weitere Auftragsverarbeiter/Ort der Verarbeitung

(1) Die Verarbeitung der Daten im Auftrag erfolgt nur in den Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR). Eine Verarbeitung der personenbezogenen Daten in einem Drittland kommt nur in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44– 49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.

(2) Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter nach Art. 28 DSGVO einzusetzen, um den Vertrag zu erfüllen.

(3) Die weiteren Auftragsverarbeiter, die derzeit eingesetzt werden, sind in Anlage 3 zu diesem Vertrag aufgeführt. Der Auftraggeber willigt in ihren Einsatz ein.

(4) Der Auftragsverarbeiter wird den Auftraggeber unterrichten, wenn er andere Subunternehmer einzusetzen wünscht. Der Auftraggeber kann diese ablehnen, wenn dafür ein wichtiger Grund besteht. Ist dem Auftragsverarbeiter aufgrund der Ablehnung eines neuen Subunternehmers die Erfüllung des Vertrages nicht mehr zumutbar, kann er den Hauptvertrag innerhalb einer angemessenen Frist kündigen.

(5) Die Unterrichtung des Auftraggebers über neue oder ersetzte Unterauftragsverarbeiter kann auch in Textform, per E-Mail, über die Plattform, über eine im Hauptvertrag benannte Kontaktadresse oder durch Aktualisierung einer dem Auftraggeber zugänglichen Übersicht erfolgen. Der Auftraggeber kann innerhalb einer angemessenen Frist aus wichtigem Grund widersprechen.

(6) Der Auftragsverarbeiter ist verpflichtet, die Pflichten aus diesem Vertrag auf die Subunternehmer zu übertragen.

(7) Subunternehmer im Sinne dieser Regelung sind nur solche Unternehmen, die Dienstleistungen unmittelbar in Bezug auf die Hauptleistung des Vertrages beziehen. Davon sind insbesondere Nebenleistungen wie Telekommunikations-, Druck- und Transportleistungen ebenso ausgenommen wie Pflichten zu reiner Wartung, die Entsorgung von Datenträgern sowie Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der personenbezogenen Daten, Netze, Dienste, Datenverarbeitungsanlagen und sonstiger IT- Systeme. Unberührt bleibt die Verpflichtung des Auftragsverarbeiters, Datenschutz und Datensicherheit in Bezug auf die Daten des Auftraggebers sicher zu stellen.

§ 9 Haftung und Schadensersatz

(1) Macht ein Betroffener Schadensersatzansprüche gegen eine Vertragspartei geltend, unterstützen sich die Parteien und tragen gemeinsam zur Aufklärung des Sachverhalts bei.

(2) Auftragsverarbeiter und Auftraggeber haften nach Maßgabe des Art. 82 DSGVO für Schäden, die eine betroffene Person aufgrund einer rechtlich nicht zulässigen oder unrichtigen Datenverarbeitung in diesem Auftragsverhältnis erleidet.

§ 10 Schlussbestimmungen

(1) Für Streitschlichtung, Rechtswahl und Gerichtsstand gilt der Hauptvertrag.

(2) Dieser Vertrag ist in Textform geschlossen und bedarf zu seiner Änderung der Textform.

- Anlage 1 – betroffene Daten- und Personengruppen

- Anlage 2 – technische und organisatorische Maßnahmen
- Anlage 3 – Subunternehmer

Anlage 1 - Betroffene Daten- und Personengruppen

Der Auftragsverarbeiter bietet eine Software an, die Unternehmen dabei unterstützt, geschäftsbezogene Informationen, Beziehungen, Kommunikation, Meetings, Dokumente und operative Prozesse in einem zentralen Workspace zu organisieren, zu strukturieren und mithilfe von Künstlicher Intelligenz (KI) zu analysieren und zu unterstützen.

Die Hauptfunktionen der Software umfassen insbesondere die Verwaltung von Personen und Unternehmen, Meetings, Notizen, Dokumenten, Kommunikationshistorien, Aufgaben, Workflows, Boards, Schnittstellen und Automatisierungen. Die Software kann außerdem Module für synchrone und asynchrone Kommunikation umfassen, insbesondere FlowListnr für Meetings, Calls, Transkription und Zusammenfassungen sowie FlowWritr für Chat-, Messaging- und Kommunikationskontexte, soweit diese vom Auftraggeber gebucht, aktiviert oder genutzt werden.

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen

| Personalstammdaten (zB Anrede, Nachname, Vorname, Anschrift, Titel, Beruf)
Kommunikationsdaten (z. B. E-Mail-Adresse, Telefonnummer, Chat- oder Messenger-Kennung, Kommunikationshistorie) Vertragsstammdaten (zB Vertragsbeziehungen, Produkt- und Vertragsinteressen) Kundenhistorie und Beziehungsdaten (zB Leads, Interessentenstatus)
Daten, die Nutzer in Nachrichten, Freitextfeldern, Notizen, Dokumenten, Dateien oder sonstigen Inhalten von sich aus übermitteln | Zweck: Bereitstellung und Betrieb der ConnectWunder-Software Organisation und Strukturierung von Geschäftsbeziehungen, Kontakten, Kommunikation, Meetings, Dokumenten und operativen Prozessen Unterstützung von Vertrieb, Kundenbetreuung, Account Management, Support, interner Zusammenarbeit und sonstigen geschäftlichen Abläufen Bereitstellung einer zentralen Kontextschicht für geschäftsbezogene Informationen KI-gestützte Analyse, Strukturierung, Zusammenfassung und Generierung von Inhalten Art: Erfassung, Organisation, Speicherung, Anordnung, Anpassung oder Veränderung, Abfrage, Verwendung, Abgleich, Einschränkung, Löschung von Daten. | Nutzer und Mitarbeiter des Auftraggebers Kunden des Auftraggebers Interessenten und Leads des Auftraggebers Geschäftspartner, Kontaktpersonen, Dienstleister und sonstige Kommunikationspartner des Auftraggebers |

| Bei Nutzung von FlowListnr zusätzlich: - Meeting- und Gesprächsdaten (z. B. Meetinginformationen, Teilnehmerdaten, Gesprächsinhalte, Notizen, Protokolle, Zusammenfassungen) - Audioaufzeichnungen oder Audiodaten, soweit solche durch den Auftraggeber erfasst, aktiviert oder eingebracht werden - Transkripte sowie daraus abgeleitete Zusammenfassungen, Aufgaben, Erkenntnisse oder Meeting-Artefakte | Zweck: - Vorbereitung, Erfassung, Transkription, Strukturierung und Nachbereitung von Meetings oder Calls - Erstellung von Zusammenfassungen, Aufgaben, Erkenntnissen oder sonstigen Meeting-Artefakten Art: - Erfassung, Speicherung, Transkription, Organisation, Strukturierung, Analyse, Verwendung, Bereitstellung, Übermittlung, Einschränkung und Löschung von Daten | - Nutzer und Mitarbeiter des Auftraggebers - Teilnehmer von Meetings, Calls oder sonstigen Gesprächen - Kunden, Interessenten, Geschäftspartner oder sonstige Gesprächspartner des Auftraggebers |

| Bei Nutzung von FlowWritr zusätzlich: - Chat-, Messaging- und Kommunikationsinhalte - Sprachnachrichten, Bilder, Medien, Anhänge oder Dateien, soweit diese durch den Auftraggeber eingebracht oder angebunden werden - Empfänger- und Absenderdaten -Kommunikations- metadaten - Nachrichtenentwürfe, Vorschläge und ggf. Writeback-Daten | Zweck: - Verarbeitung, Strukturierung und Bereitstellung von Chat-, Messaging- und Kommunikationskontexten - Erstellung von Nachrichtenentwürfen, Vorschlägen oder Kommunikationshistorien - Übermittlung oder Rückübertragung von Kommunikationsinhalten in angebundene Systeme oder Kommunikationskanäle, soweit vom Auftraggeber aktiviert oder angewiesen Art: - Erfassung, Speicherung, Organisation, Strukturierung, Analyse, Verwendung, Bereitstellung, Übermittlung, Abgleich, Einschränkung und Löschung von Daten | - Nutzer und Mitarbeiter des Auftraggebers - Chat-Partner, Empfänger von Nachrichten, Kunden, Interessenten, Geschäftspartner oder sonstige Kommunikationspartner des Auftraggebers |

| Technische Daten (IP-Adresse, Log-Daten, Bestell-ID) | Zweck: Technische Unterstützung, Wartung, Sicherheit, Fehleranalyse und Betrieb der Plattform Art: Erhebung, Erfassung, Organisation, Speicherung, Anordnung, Anpassung oder Veränderung, Abfrage, Verwendung,

Abgleich, Einschränkung, Löschung von Daten. | Nutzer und Mitarbeiter des Auftraggebers sonstige Personen, deren Daten im Rahmen der Nutzung technisch verarbeitet werden |

Besondere Kategorien personenbezogener Daten:

Die ConnectWunder-Software ist nicht darauf ausgelegt, besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO gezielt zu verarbeiten. Da der Auftraggeber Inhalte in Form von Kommunikation, Meetings, Chats, Audio, Medien, Dokumenten oder Freitexten selbst in die Plattform einbringen oder anbinden kann, kann nicht ausgeschlossen werden, dass solche Daten durch den Auftraggeber oder dessen Kommunikationspartner in die Plattform eingebracht werden. Der Auftraggeber stellt sicher, dass solche Daten nur verarbeitet werden, wenn dies rechtlich zulässig ist und geeignete Schutzmaßnahmen getroffen wurden.

Anlage 2 - technische und organisatorische Maßnahmen zum Schutz der Daten

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

- Zugangskontrollen: Persönlicher und individueller Login, Firewall
- Zugriffskontrollen: Verschlüsselung von Datenträgern
- Zugriff auf personenbezogene Daten durch Nutzer des Auftraggebers entsprechend der vom Auftraggeber innerhalb des Workspaces vergebenen Berechtigungen
- Eingeschränkte Besucherzugriffe auf einzelne Dokumente oder Boards, soweit technisch vorgesehen
- Administrative Zugriffe durch den Auftragsverarbeiter nur, soweit dies für Betrieb, Support, Sicherheit oder Fehlerbehebung erforderlich ist

Trennungskontrollen:

- Trennung von Entwicklungs- und Produktionsumgebung
- Arbeits-Computer: Verwendung von verschlüsselten Verbindungen für den Zugriff auf Cloud-Dienste;
- Cloud-Dienste: Logische Trennung der Systeme durch verschiedene Mandantenfähigkeiten der IT-Systeme; Nutzung von Cloud-Diensten, die eine sichere und getrennte Verarbeitung von Daten ermöglichen.
- Logische Trennung von Workspaces und Daten verschiedener Auftraggeber innerhalb der Plattform

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

- Verschlüsselung von Datenträgern
- Gesicherter File Transfer oder sonstiger Datentransport
- Schutz vor unbefugter Veränderung durch Zugriffsrechte und Berechtigungskonzepte

Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Zugriffsrechte
- Systemseitige Protokollierungen
- Protokollierung sicherheitsrelevanter Ereignisse und Änderungen, soweit technisch vorgesehen

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO):

- regelmäßige Backups
- Für die Verfügbarkeit und Belastbarkeit der Daten, die bei Google Cloud, Firebase, OpenAI oder sonstigen in Anlage 3 aufgeführten Subunternehmern gespeichert oder verarbeitet werden, verweisen wir auf die technischen und organisatorischen Maßnahmen dieser Anbieter.

Auftragskontrolle:

- Vereinbarung zur Auftragsverarbeitung
- Kontrolle der Auftragsdurchführung
- Auswahl von Subunternehmern unter Berücksichtigung geeigneter Datenschutzgarantien
- Vertragliche Verpflichtung von Subunternehmern auf datenschutzrechtliche Pflichten

Zusätzliche Schutzmaßnahmen bei Kommunikationsdaten

Soweit der Auftraggeber Kommunikationsfunktionen, Meeting-Funktionen, Call-Funktionen, Messaging-Funktionen, Transkription, Medienverarbeitung oder Writeback-Funktionen nutzt,

gelten zusätzlich folgende Schutzmaßnahmen:

- Zugriff auf Kommunikationsinhalte erfolgt nur im für die Bereitstellung, Wartung, Sicherheit, Fehleranalyse oder den Support der Plattform erforderlichen Umfang.
- Audio-, Transkript-, Nachrichten-, Medien- und Meetingdaten werden nur im Rahmen der Plattformfunktionalität und nach Maßgabe der Weisungen des Auftraggebers verarbeitet.
- Administrative Zugriffe auf Kommunikationsinhalte werden auf erforderliche Support-, Sicherheits-, Betriebs- oder Fehlerbehebungsfälle beschränkt.
- Transkripte, Nachrichten, Medien und Meeting-Artefakte werden innerhalb der Plattform unter Nutzung der vorgesehenen Authentifizierungs-, Berechtigungs- und Transportverschlüsselungsmechanismen verarbeitet.
- Rohtranskripte oder vergleichbare Verarbeitungseingaben können, soweit technisch vorgesehen, vorübergehend zur Verarbeitung gespeichert werden. Eine dauerhafte Speicherung erfolgt nur, soweit dies Teil der jeweiligen Plattformfunktionalität ist oder vom Auftraggeber entsprechend konfiguriert wurde.
- Aus Rohtranskripten, Nachrichten oder Meetingdaten abgeleitete Inhalte, insbesondere Zusammenfassungen, Notizen, Aufgaben, Entscheidungen, Dokumente oder sonstige Meeting-Artefakte, können als reguläre Plattformdaten gespeichert werden.
- Versand, Synchronisierung oder Writeback in angebundene Systeme oder Kommunikationskanäle erfolgt nur, soweit der Auftraggeber die jeweilige Integration, den Trigger, Agenten oder eine sonstige Automatisierung bewusst eingerichtet oder eine konkrete Aktion manuell ausgelöst hat, und nur im technisch vorgesehenen Leistungsumfang.

Ergänzend bleibt der Auftraggeber für die rechtmäßige Einrichtung, Konfiguration und Nutzung von Kommunikations-, Transkriptions-, Medienverarbeitungs-, Integrations- und Writeback-Funktionen verantwortlich, insbesondere für erforderliche Informationspflichten, Einwilligungen und Berechtigungen gegenüber betroffenen Personen sowie für erforderliche Zugriffsrechte, Freigaben und Konfigurationen im Zusammenhang mit angebotenen Drittplattformen.

Verweis auf technische und organisatorische Maßnahmen von Subunternehmern:

- Die Verfügbarkeit, Integrität und Sicherheit der Daten, die bei Google Cloud, Firebase, OpenAI oder sonstigen in Anlage 3 aufgeführten Subunternehmern gespeichert oder verarbeitet werden, unterliegen den technischen und organisatorischen Maßnahmen dieser Anbieter. Weitere Details zu diesen Maßnahmen sind in den jeweiligen Sicherheitsdokumentationen, Datenschutzrichtlinien oder Datenverarbeitungsvereinbarungen der Anbieter verfügbar.

Referenzdokumentationen der Subunternehmer:

1. Google Cloud & Firebase:

1. Sicherheitsdokumentation: <https://cloud.google.com/trust-center/security?hl=en>
(<https://cloud.google.com/trust-center/security?hl=en>)
2. Datenschutzrichtlinie: Google Cloud Privacy (<https://cloud.google.com/privacy>)
3. Cloud Data Processing Addendum <https://cloud.google.com/terms/data-processing-addendum>
(<https://cloud.google.com/terms/data-processing-addendum>)
4. Verschlüsselungsmaßnahmen und Zertifikate des Rechenzentrums:
<https://cloud.google.com/docs/security/encryption/default-encryption>
(<https://cloud.google.com/docs/security/encryption/default-encryption>)
<https://cloud.google.com/security/compliance/iso-27001/>
(<https://cloud.google.com/security/compliance/iso-27001/>)

2. OpenAI:

1. Sicherheitsdokumentation: OpenAI Security (<https://openai.com/security>)
2. Datenschutzrichtlinie: OpenAI Privacy (<https://openai.com/privacy>)

3. ElevenLabs:

1. Sicherheitsdokumentation / Trust Center: <https://compliance.elevenlabs.io/>
(<https://compliance.elevenlabs.io/>)
2. Datenschutzrichtlinie: <https://elevenlabs.io/privacy-policy>
(<https://elevenlabs.io/privacy-policy>)
3. Data Processing Addendum: <https://elevenlabs.io/dpa> (<https://elevenlabs.io/dpa>)

Anlage 3 – Subunternehmer im Rahmen der Auftragsverarbeitung

| Name und Anschrift des Subunternehmers | Beschreibung der Teilleistungen |

| ----- | ----- |

| Google Firebase 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA | Speicherung von Nutzerdaten und Interaktionsdaten in der Cloud-Region Europa |

| Google Cloud 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA | Produktbereitstellung durch Produkt-Hosting in der Cloud-Region Europa. |

| OpenAI 3180 18th Street, San Francisco, CA 94110, USA | KI-gestützte Verarbeitung, Analyse, Strukturierung, Zusammenfassung und Generierung von Inhalten sowie Beantwortung von Nutzeranfragen, soweit OpenAI für die jeweilige Funktion eingesetzt wird. |

| ElevenLabs Eleven Labs Inc., 169 Madison Ave #2484, New York, NY 10016, USA | KI-gestützte Audioverarbeitung, insbesondere Transkription, Analyse und Verarbeitung von Audioinhalten, soweit ElevenLabs für die jeweilige Funktion eingesetzt wird. |

Soweit Unterauftragsverarbeiter außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums eingesetzt werden oder ein Zugriff aus einem Drittland erfolgt, erfolgt dies nur unter Einhaltung der gesetzlichen Anforderungen der Art. 44 bis 49 DSGVO, insbesondere durch geeignete Garantien wie Standardvertragsklauseln oder andere gesetzlich vorgesehene Schutzmechanismen.