Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zu den Allgemeinen Geschäftsbedingungen der novendix GmbH

Stand: November 2026 – Version 1.12

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") konkretisiert die datenschutzrechtlichen Pflichten der novendix GmbH (nachfolgend „Auftragsverarbeiter") gegenüber dem Kunden (nachfolgend „Verantwortlicher") gemäß Art. 28 DSGVO, soweit der Auftragsverarbeiter im Rahmen der Erbringung der vertraglich vereinbarten Leistungen (Plattform-Nutzung gemäß den Allgemeinen Geschäftsbedingungen der novendix GmbH, nachfolgend „Hauptvertrag") personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Dieser AVV gilt ergänzend zum Hauptvertrag. Im Falle von Widersprüchen zwischen diesem AVV und dem Hauptvertrag geht dieser AVV hinsichtlich der Verarbeitung personenbezogener Daten vor.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

1.1 Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit der Bereitstellung und dem Betrieb der novendix-Plattform (KI-gestützte Assistenz- und Automatisierungsplattform) gemäß Hauptvertrag. Die Plattform wird sowohl webbasiert als auch über die vom Auftragsverarbeiter bereitgestellten nativen Anwendungen für Android und iOS/iPadOS („Apps“) bereitgestellt; dieser AVV gilt für beide Zugangswege gleichermaßen.

1.2 Die Verarbeitung umfasst insbesondere das Speichern, Übermitteln, Auslesen, Verarbeiten und Löschen personenbezogener Daten, die der Verantwortliche bzw. die von ihm autorisierten Nutzer im Rahmen der Nutzung der Plattform eingeben, hochladen oder generieren (z. B. Chat-Verläufe, hochgeladene Dokumente, Nutzerkonto-Daten).

1.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Nach Beendigung des Hauptvertrags gelten die Lösch- und Rückgabepflichten gemäß § 8 dieses AVV. Während der Laufzeit des Hauptvertrags bestimmt der Verantwortliche die Speicherdauer der Inhaltsdaten nach Maßgabe von § 8.1.

1.4 Zweck der Verarbeitung ist ausschließlich die Erbringung der im Hauptvertrag vereinbarten Leistungen. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters, insbesondere zum Training von KI-Modellen mit Kundendaten, findet nicht statt. Unberührt bleibt die Erstellung anonymisierter, aggregierter Betriebsstatistiken (z. B. Auslastung, Modellnutzung, Fehlerraten) ohne Personen-, Kunden- oder Inhaltsbezug zum Betrieb, zur Sicherheit und zur Weiterentwicklung der Plattform.

§ 2 Kategorien betroffener Personen und Daten

2.1 Kategorien betroffener Personen: Mitarbeiter, Beauftragte und sonstige Nutzer des Verantwortlichen, die die Plattform im Rahmen ihrer Tätigkeit für den Verantwortlichen nutzen, sowie ggf. Dritte, deren personenbezogene Daten von diesen Nutzern in die Plattform eingegeben werden (z. B. Ansprechpartner in Kundendokumenten).

2.2 Kategorien personenbezogener Daten: Kontakt- und Stammdaten (Name, E-Mail-Adresse), Nutzungs- und Protokolldaten (Login-Zeiten, IP-Adressen), Inhalte, die von Nutzern in die Plattform eingegeben, hochgeladen oder durch die Nutzung generiert werden (z. B. Texte, Dokumente, Chat-Inhalte), Transkripte und Zusammenfassungen aufgezeichneter Besprechungen, von der Plattform gespeicherte Personalisierungsangaben zu einzelnen Nutzern, Gerätekennungen für mobile Benachrichtigungen sowie verschlüsselt gespeicherte Zugangsdaten zu den vom Nutzer verbundenen Drittsystemen, soweit diese personenbezogene Daten enthalten.

Hinzu kommen die Identitäts- und Anmeldedaten des vom Auftragsverarbeiter selbst betriebenen Identitätsdienstes (Benutzerkennung, Passwort-Hash, Sitzungen, Rollenzuweisungen) sowie die organisationsbezogenen Verbrauchs- und Budgetdaten der Modellnutzung.

2.3 Der Verantwortliche ist allein dafür verantwortlich, dass die von ihm bzw. seinen Nutzern in die Plattform eingegebenen Daten rechtmäßig verarbeitet werden dürfen und keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) eingegeben werden, es sei denn, dies wurde gesondert schriftlich vereinbart.

§ 3 Verarbeitungsstandort

3.1 Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Die Plattform und ihre Datenbanken werden in Rechenzentren in Deutschland betrieben. Dies gilt ebenso für die kundenspezifischen Container-Umgebungen, über die die App- und MCP-Anbindungen bereitgestellt werden. Die zusätzliche, verschlüsselte Sicherung der Datenbanken und Dateien wird in einem räumlich getrennten Rechenzentrum in Frankfurt am Main abgelegt. Ein Ersatzsystem, auf das die Produktivumgebung regelmäßig gespiegelt wird und das bei einem schwerwiegenden Ausfall den Betrieb übernehmen kann, wird bei der Hetzner Online GmbH in Deutschland vorgehalten. Näheres regelt Anlage 1, Abschnitt 5.2. Einzelne Zusatzfunktionen übermitteln Daten in Drittländer; diese sind in § 5.5 benannt. Über die Aufnahme weiterer Verarbeitungen außerhalb der Europäischen Union informiert der Auftragsverarbeiter nach Maßgabe von § 5.2.

3.2 Der Einsatz von Subunternehmern mit Sitz oder Verarbeitungsstandort außerhalb der EU/des EWR steht unter dem Vorbehalt, dass die Voraussetzungen der Art. 44 ff. DSGVO (insbesondere Angemessenheitsbeschluss oder Standardvertragsklauseln) erfüllt sind. Der Verantwortliche wird hierüber im Rahmen der Subunternehmer-Übersicht gemäß § 5 informiert.

3.3 Die Verwaltung der Identitäten und Anmeldungen, die Erzeugung und Bearbeitung von Dokumenten, Tabellen, Präsentationen und PDF-Dateien, die Spracherkennung und Transkription einschließlich der Diktierfunktion im Chat, der Aufzeichnung von Besprechungen und des Besprechungsassistenten für Microsoft Teams und Google Meet sowie das Abrufen von Webseiten im Rahmen der Recherchefunktion erfolgen auf den Servern des Auftragsverarbeiters in Deutschland. Für diese Verarbeitungsschritte selbst werden keine personenbezogenen Daten an Dritte übermittelt; insbesondere werden Audiodaten an keinen externen Sprachdienstleister übermittelt. Wird ein auf diesem Weg erzeugter Text – etwa eine Transkription oder der Inhalt einer abgerufenen Webseite – anschließend zusammengefasst, ausgewertet oder in anderer Weise durch ein Sprachmodell verarbeitet, so erfolgt dieser weitere Schritt über den Modell-Gateway nach § 5.4; Satz 2 Halbsatz 1 gilt insoweit nicht.

§ 4 Weisungsgebundenheit und Vertraulichkeit

4.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zu einer anderweitigen Verarbeitung verpflichtet; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2 Der Hauptvertrag nebst diesem AVV stellt die erste dokumentierte Weisung des Verantwortlichen dar. Weitere Weisungen sind in Textform gegenüber der vom Auftragsverarbeiter benannten Kontaktstelle zu erteilen und werden vom Auftragsverarbeiter dokumentiert.

4.3 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt, wird er den Verantwortlichen unverzüglich informieren. Der Auftragsverarbeiter ist berechtigt, die Umsetzung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

4.4 Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten des Verantwortlichen befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; die Verpflichtung gilt über das Ende ihrer Tätigkeit hinaus fort. Der Zugriff auf personenbezogene Daten wird auf das für die jeweilige Aufgabe erforderliche Maß beschränkt. Für Subunternehmer gilt § 5.3.

§ 5 Subunternehmer

5.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zum Einsatz der nachfolgend genannten Subunternehmer (Unterauftragsverarbeiter):

Subunternehmer	Funktion	Verarbeitungsstandort	Land
Hetzner Online GmbH	Hosting der Plattform-Infrastruktur (Server, Datenbanken), der kundenspezifischen Container-Umgebungen für die App- und MCP-Anbindungen sowie des Ersatzsystems	Rechenzentren in Deutschland	Deutschland
BES Systemhaus GmbH; Weiterverlagerung an Wasabi Technologies, Inc. bzw. die zuständige Wasabi-Vertragsgesellschaft	Verschlüsselte Speicherung der täglichen Datensicherung; das Schlüsselmaterial verbleibt beim Auftragsverarbeiter. Der Speicher wird über BES Systemhaus GmbH bezogen. Auftragsverarbeitungsverträge bestehen zwischen dem Auftragsverarbeiter und BES Systemhaus GmbH sowie zwischen BES Systemhaus GmbH und Wasabi. Einzelheiten in Anlage 1, Abschnitt 5.2.	Rechenzentrum in Frankfurt am Main	Deutschland (Muttergesellschaft USA; Standardvertragsklauseln, § 5.5)
Requesty Ltd, London	KI-Modell-Gateway; Weiterleitung der Anfragen an die Sprach- und Bildmodell-Anbieter nach § 5.4	Verarbeitung über den EU-Endpunkt	Vereinigtes Königreich (Angemessenheitsbeschluss der EU-Kommission)
BES Systemhaus GmbH	Anwendersupport und Zuarbeiten bei der Systemadministration im Auftrag des Auftragsverarbeiters; Zugriff auf Systeme und Daten nur im Rahmen dieser Unterstützung; Bezug des Objektspeichers für die tägliche Sicherung nach Zeile 2 dieser Aufstellung.	Deutschland (Schwabach)	Deutschland
Lexware Office (Haufe-Lexware GmbH & Co. KG)	Rechnungsstellung und Buchhaltung; nicht an der Verarbeitung von Plattforminhalten beteiligt	Deutschland	Deutschland
mittwald CM Service GmbH & Co. KG	Hosting der Website novendix.ai; nicht an der Verarbeitung von Plattforminhalten beteiligt	Deutschland	Deutschland
IONOS SE	Domainverwaltung (Registrierung und Nameserver); nicht am Versand von E-Mails und nicht an der Verarbeitung von Plattforminhalten beteiligt	Deutschland	Deutschland
Microsoft Ireland Operations Ltd.	Versand der System-E-Mails der Plattform und der Website (u. a. Registrierung, Passwort-Zurücksetzen, Benachrichtigungen, Bestätigungen zu Formularen) über den Microsoft-365-Mandanten des Auftragsverarbeiters;	Europäische Union (EU Data Boundary)	Irland (Muttergesellschaft USA; Standardvertragsklauseln im Microsoft-

Subunternehmer	Funktion	Verarbeitungsstandort	Land
	Betrieb des Kontos, mit dem der Besprechungsassistent des Auftragsverarbeiters an Microsoft-Teams-Besprechungen des Verantwortlichen teilnimmt		Datenschutznachtrag, EU-US Data Privacy Framework)
Linkup Technologies SAS	Websuche; erhält die Suchanfrage, sofern ein Nutzer die Websuche verwendet; hierüber werden auch Wetterfragen beantwortet	Verarbeitungsregion Europäische Union	Frankreich (Subunternehmer mit Sitz in den USA; Standardvertragsklauseln, § 5.5)
Pipedream, Inc.	Vermittlung der vom Nutzer selbst eingerichteten App-Verbindungen (u. a. Outlook, Gmail, OneDrive)	USA	Drittland (§ 5.5)
Pexels (Canva)	Bildsuche bei der automatischen Erstellung von Präsentationen; übermittelt werden ausschließlich ein bis drei allgemeine englische Motivbegriffe; der Bildabruf erfolgt über die Server des Auftragsverarbeiters	Australien / USA	Drittland; keine Übermittlung personenbezogener Daten (§ 5.5)
Google Ireland Limited (Firebase Cloud Messaging; Google Meet)	Zustellung von Push-Benachrichtigungen an Android-Geräte; übermittelt werden der Push-Token des Geräts sowie Inhalt und Zeitpunkt der Benachrichtigung; Betrieb des Kontos, mit dem der Besprechungsassistent des Auftragsverarbeiters an Google-Meet-Besprechungen des Verantwortlichen teilnimmt	Irland; Zustellinfrastruktur weltweit	EU, Drittlandübermittlung nicht ausgeschlossen (§ 5.5)
Apple Distribution International Ltd. (Apple Push Notification service)	Zustellung von Push-Benachrichtigungen an Geräte mit iOS und iPadOS; übermittelt werden der Push-Token des Geräts sowie Inhalt und Zeitpunkt der Benachrichtigung	Irland; Zustellinfrastruktur weltweit	EU, Drittlandübermittlung nicht ausgeschlossen (§ 5.5)

5.2 Der Auftragsverarbeiter wird den Verantwortlichen über die Hinzuziehung oder Ersetzung weiterer Subunternehmer mit einer Frist von mindestens vierzehn (14) Tagen vor der geplanten Änderung in Textform informieren; die Information an die vom Verantwortlichen zuletzt benannte Kontaktadresse genügt. Der Verantwortliche kann der Änderung innerhalb von zehn (10) Tagen nach Zugang der Information aus wichtigem, datenschutzrechtlich begründetem Grund widersprechen. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Änderung als genehmigt. Beim Wechsel eines Subunternehmers innerhalb derselben Funktion, der weder den Verarbeitungsort verändert noch eine neue Übermittlung in ein Drittland begründet, beträgt die Frist nach Satz 1 sieben (7) Tage; der Verantwortliche kann innerhalb dieser Frist nach Satz 2 widersprechen. Ist eine Hinzuziehung oder Ersetzung erforderlich, um eine erhebliche Störung der Verfügbarkeit oder Sicherheit der Plattform abzuwenden oder zu beheben, oder um den Ausfall oder die kurzfristige Beendigung der Leistungen eines bisherigen Subunternehmers zu überbrücken, ist der Auftragsverarbeiter berechtigt, die Änderung ohne Einhaltung der Vorlauffrist vorzunehmen; er informiert den Verantwortlichen in diesem Fall unverzüglich nach der Änderung in Textform, und das Widerspruchsrecht nach Satz 2 kann innerhalb von zehn (10) Tagen nach Zugang dieser Information ausgeübt werden. Bei einem berechtigten Widerspruch werden die Parteien eine einvernehmliche Lösung suchen; gelingt dies nicht innerhalb einer angemessenen Frist, ist der Verantwortliche berechtigt, den Hauptvertrag außerordentlich zu kündigen, soweit ihm die Fortsetzung der Zusammenarbeit unter Einbeziehung des neuen Subunternehmers unzumutbar ist.

5.3 Der Auftragsverarbeiter wird alle Subunternehmer im Wege einer Vereinbarung, die inhaltlich den Anforderungen des Art. 28 Abs. 2 bis 4 DSGVO entspricht, zur Einhaltung der einschlägigen datenschutzrechtlichen Pflichten verpflichten.

5.4 Die Sprach- und Bildmodelle sowie die Modelle zur Vektorisierung von Texten (Embeddings) werden nicht unmittelbar, sondern über den in § 5.1 genannten Modell-Gateway bezogen. Über diesen werden derzeit Modelle von Anthropic, OpenAI, Microsoft (Azure OpenAI), Google (Vertex AI), Mistral AI und Amazon Web Services (Bedrock) eingesetzt. Die Anfragen werden zunächst über einen vom Auftragsverarbeiter selbst betriebenen, auf dessen Servern in Deutschland laufenden Modell-Proxy geführt; von dort laufen sämtliche Anfragen über den als EU gekennzeichneten Endpunkt des Gateway-Anbieters. Die Anfragen an Sprachmodelle und an die Modelle zur Vektorisierung von Texten werden ausschließlich an Modellvarianten mit Verarbeitung in Rechenzentren innerhalb der Europäischen Union geleitet. Für die Bildmodelle weist der Gateway-Anbieter keine auf die Europäische Union festgelegte Verarbeitungsregion aus; insoweit gilt § 5.5 Buchstabe (f). Für alle über den Gateway bezogenen Modelle ist vereinbart, dass die übermittelten Inhalte nicht zum Training von Modellen verwendet und weder beim Gateway-Anbieter noch beim Modellanbieter gespeichert werden (Zero Retention); Modelle ohne diese Zusicherung werden vom Gateway abgelehnt. Für die Verpflichtung dieser mittelbar beauftragten Anbieter gilt § 5.3 entsprechend. Die Hinzunahme oder Ersetzung eines Modellanbieters nach Satz 2 teilt der Auftragsverarbeiter dem Verantwortlichen nach Maßgabe von § 5.2 mit. Neue Modelle oder Modellversionen eines bereits genannten Anbieters sowie der Wegfall eines Anbieters bedürfen keiner Mitteilung nach § 5.2.

5.5 Folgende Verarbeitungen können außerhalb der Europäischen Union stattfinden: (a) die Übermittlung der Suchanfrage an Linkup, sofern ein Nutzer die Websuche verwendet; hierüber werden auch Wetterfragen beantwortet. Die Verarbeitung erfolgt in der Verarbeitungsregion Europäische Union; diese gilt nach dem mit Linkup geschlossenen Auftragsverarbeitungsvertrag als Voreinstellung, und die Verarbeitungsregion Vereinigte Staaten wurde nicht gewählt. Linkup setzt seinerseits Subunternehmer ein, darunter zwei mit Sitz in den Vereinigten Staaten (Protokollierung und Überwachung sowie Anreicherung des Suchindex); für Übermittlungen an Subunternehmer außerhalb des Europäischen Wirtschaftsraums bindet dieser Vertrag die Standardvertragsklauseln der Europäischen Kommission (Modul 3) ein; (b) die Übermittlung von Verbindungsdaten und Zugangstoken an Pipedream, sofern ein Nutzer eine App-Verbindung einrichtet; (c) die Übermittlung von ein bis drei allgemeinen englischen Bildsuchbegriffen an Pexels, sofern bei der automatischen Erstellung einer Präsentation eine Bildfolie vorgesehen ist; die Begriffe werden technisch auf allgemeine Motivbeschreibungen ohne Namen von Personen, Unternehmen, Produkten oder Projekten begrenzt. Chatverläufe, Folientexte, hochgeladene Dateien sowie Nutzer- und Organisationsdaten werden nicht übermittelt; der Bildabruf erfolgt über die Server des Auftragsverarbeiters, sodass auch die IP-Adressen der Nutzer nicht übermittelt werden; (d) die Übermittlung des Push-Tokens sowie des Inhalts und des Zeitpunkts einer Benachrichtigung an Google (Firebase Cloud Messaging), sofern ein Nutzer Push-Benachrichtigungen auf einem Android-Gerät zulässt; (e) die Übermittlung des Push-Tokens sowie des Inhalts und des Zeitpunkts einer Benachrichtigung an Apple (Apple Push Notification service), sofern ein Nutzer Push-Benachrichtigungen auf einem Gerät mit iOS oder iPadOS zulässt; (f) die Übermittlung der Bildbeschreibung an die Bildmodelle von Microsoft (Azure OpenAI) bzw. Google (Vertex AI) über den Modell-Gateway, sofern ein Nutzer ein Bild erzeugen lässt. Für diese Modelle weist der Gateway-Anbieter keine auf die Europäische Union festgelegte Verarbeitungsregion aus. Übermittelt wird ausschließlich der Text der Bildbeschreibung, nicht der Gesprächsverlauf, nicht hochgeladene Dateien und keine Nutzerkennung. Vor der Übermittlung wird der Text automatisiert auf personenbezogene Daten geprüft (Regelwerk für E-Mail-Adressen, Telefonnummern, IBAN, Kreditkartennummern, Anschriften und Geburtsdaten sowie eine ergänzende Prüfung durch ein Sprachmodell mit Verarbeitung in der Europäischen Union); bei einem Treffer oder bei einem Ausfall der Prüfung unterbleibt die Übermittlung und der Nutzer erhält einen Hinweis. Für die eingesetzten Bildmodelle ist zugesichert, dass die übermittelten Inhalte nicht gespeichert und nicht zum Training verwendet werden. Vertragspartner für (d) und (e) sind die in § 5.1 genannten Gesellschaften mit Sitz in Irland; eine Übermittlung in Drittländer im Rahmen der

weltweiten Zustellinfrastruktur dieser Anbieter ist nicht ausgeschlossen. Für die Übermittlungen nach (a), (b), (d), (e) und (f) werden die Standardvertragsklauseln der Europäischen Kommission zugrunde gelegt; Microsoft und Google sind zusätzlich unter dem EU-US Data Privacy Framework zertifiziert. Bei der Übermittlung nach (c) werden keine personenbezogenen Daten übermittelt. Die Funktionen nach (a), (b), (d), (e) und (f) sind optional und werden nur auf Veranlassung bzw. mit ausdrücklicher Zustimmung des jeweiligen Nutzers ausgelöst. Der Gateway-Anbieter Requesty Ltd hat seinen Sitz im Vereinigten Königreich, für das ein Angemessenheitsbeschluss der Europäischen Kommission besteht; die Anfragen werden über dessen EU-Endpunkt verarbeitet. Die Muttergesellschaft des Speicheranbieters Wasabi Technologies hat ihren Sitz in den USA; der über BES Systemhaus GmbH geschlossene Vertrag mit Wasabi bindet die Standardvertragsklauseln ein; die Daten verbleiben in der gewählten Region Frankfurt am Main, und Datensicherungen erhält der Anbieter ausschließlich verschlüsselt. Der Versand der System-E-Mails erfolgt über den Microsoft-365-Mandanten des Auftragsverarbeiters; die Verarbeitung findet innerhalb der Europäischen Union statt. Die Muttergesellschaft des Anbieters Microsoft Ireland Operations Ltd. hat ihren Sitz in den USA; der Microsoft-Datenschutznachtrag bindet die Standardvertragsklauseln ein, und Microsoft ist unter dem EU-US Data Privacy Framework zertifiziert. Weitere Verarbeitungen außerhalb der Europäischen Union finden derzeit nicht statt; über die Aufnahme weiterer Verarbeitungen außerhalb der Europäischen Union informiert der Auftragsverarbeiter nach Maßgabe von § 5.2. Übermittlungen an Ziele, die der Verantwortliche oder seine Nutzer selbst einrichten – insbesondere eigene MCP-Server, API-Werkzeuge von Assistenten, Webhooks von Workflows sowie verbundene Konten, etwa bei Microsoft 365 oder Atlassian –, erfolgen auf Weisung des Verantwortlichen. Auswahl und datenschutzrechtliche Bewertung dieser Ziele liegen in seiner Verantwortung; sie sind nicht Gegenstand der Aufstellung nach § 5.1.

§ 6 Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter trifft die in Anlage 1 zu diesem AVV beschriebenen technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Hierzu zählen insbesondere Maßnahmen zur Verschlüsselung, Zugriffs- und Zutrittskontrolle, Verfügbarkeit und Belastbarkeit der Systeme sowie zur regelmäßigen Überprüfung der Wirksamkeit der Maßnahmen.

6.2 Der Auftragsverarbeiter ist berechtigt, die TOM anzupassen, sofern das vereinbarte Schutzniveau hierdurch nicht unterschritten wird.

§ 7 Unterstützung des Verantwortlichen

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen, soweit dies möglich ist, bei der Erfüllung von dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte (Art. 12 bis 23 DSGVO).

7.2 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung, vorherige Konsultation), soweit dem Auftragsverarbeiter die hierfür erforderlichen Informationen vorliegen.

7.3 Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten des Verantwortlichen bekannt, informiert er den Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, in Textform über den Sachverhalt, die betroffenen Datenkategorien, die mutmaßlichen Auswirkungen sowie die bereits ergriffenen bzw. vorgeschlagenen Abhilfemaßnahmen.

7.4 Leistungen des Auftragsverarbeiters, die über die in diesem § 7 beschriebenen Unterstützungspflichten hinausgehen, werden gesondert nach Aufwand zu den vereinbarten bzw., in Ermangelung einer Vereinbarung, marktüblichen Preisen vergütet.

§ 8 Speicherdauer, Löschung und Rückgabe von Daten

8.1 Während der Laufzeit des Hauptvertrags speichert der Auftragsverarbeiter die Inhaltsdaten des Verantwortlichen – insbesondere Chatverläufe, hochgeladene und erzeugte Dateien, Projekte, Assistenten und gespeicherte Erinnerungen – so lange, wie der Verantwortliche dies bestimmt. Eine automatische Löschung durch den Auftragsverarbeiter findet nicht statt. Der Verantwortliche und die von ihm autorisierten Nutzer können Inhaltsdaten jederzeit selbst löschen; hierfür stehen in der Anwendung Funktionen zur Löschung einzelner Chats, sämtlicher Chats, einzelner Dateien sowie einzelner gespeicherter Erinnerungen zur Verfügung. Der Verantwortliche trägt dafür Sorge, dass die von ihm gewählte Speicherdauer dem Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO entspricht. Mit der Löschung durch den Nutzer werden die Inhalte unmittelbar aus der Anwendung entfernt und spätestens innerhalb von dreißig (30) Tagen aus sämtlichen produktiven Speicherorten gelöscht, einschließlich der primären Datenbank sowie des Volltext- und des Vektorindex. Beim Löschen eines Chats bleiben hochgeladene Dateien erhalten; sie werden im Bereich Dateien gelöscht.
8.2 Weisungen des Verantwortlichen zur Löschung einzelner Daten oder Datenbestände setzt der Auftragsverarbeiter unverzüglich um, spätestens jedoch innerhalb von dreißig (30) Tagen. Die Löschung erfasst sämtliche produktiven Speicherorte, insbesondere die primäre Datenbank, den Volltextindex der Chat- und Dateisuche sowie den Vektorindex der Dokumentensuche. Für in Datensicherungen und im Ersatzsystem enthaltene Kopien gilt § 8.5. Personenbezogene Daten im Identitätsdienst werden mit der Löschung des Kontos gelöscht; soweit dies aufgrund der Speicherart technisch nicht möglich ist, werden sie unkenntlich gemacht (anonymisiert) oder gesperrt und nicht mehr verarbeitet.
8.3 Nach Beendigung des Hauptvertrags – gleich aus welchem Grund – wird der Auftragsverarbeiter dem Verantwortlichen auf Anforderung eine Kopie der für ihn verarbeiteten personenbezogenen Daten in einem gängigen Datenformat zur Verfügung stellen.

8.4 Nach Ablauf einer Karenzzeit von einem (1) Monat nach Vertragsbeendigung löscht der Auftragsverarbeiter die personenbezogenen Daten des Verantwortlichen innerhalb von weiteren dreißig (30) Tagen, sofern keine gesetzliche Pflicht zur weiteren Aufbewahrung besteht. Die Löschung erfasst sämtliche produktiven Speicherorte, insbesondere die primäre Datenbank, den Volltextindex der Chat- und Dateisuche sowie den Vektorindex der Dokumentensuche. Der Auftragsverarbeiter weist den Verantwortlichen bei Vertragsbeendigung auf die Karenzzeit gesondert hin und bestätigt die erfolgte Löschung auf Anforderung in Textform. Personenbezogene Daten im Identitätsdienst werden mit der Löschung des Kontos gelöscht; soweit dies aufgrund der Speicherart technisch nicht möglich ist, werden sie unkenntlich gemacht (anonymisiert) oder gesperrt und nicht mehr verarbeitet.

8.5 Soweit gelöschte personenbezogene Daten noch in Datensicherungen oder im Ersatzsystem enthalten sind, werden diese Sicherungen nicht gesondert bereinigt, sondern im Rahmen des in Anlage 1 beschriebenen Sicherungszyklus überschrieben, spätestens jedoch innerhalb von sechzig (60) Tagen. Bis dahin werden die Daten nicht mehr aktiv verarbeitet. Wird eine Datensicherung innerhalb dieses Zeitraums eingespielt, werden die betroffenen Daten unverzüglich erneut gelöscht. Datensicherungen dienen der Wiederherstellung des Gesamtsystems nach einem Zwischenfall; sie begründen keinen Anspruch des Verantwortlichen auf Wiederherstellung einzelner Inhalte.

§ 9 Kontrollrechte des Verantwortlichen

9.1 Der Verantwortliche ist berechtigt, sich in geeigneter Weise, insbesondere durch Einholung von Auskünften und Vorlage aussagekräftiger Nachweise (z. B. aktuelle Testate, Berichte oder Auszüge aus Berichten unabhängiger Instanzen wie z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung,

Datenschutzauditoren, Qualitätsauditoren), von der Einhaltung der in diesem AVV vereinbarten technischen und organisatorischen Maßnahmen zu überzeugen.

9.2 Vor-Ort-Kontrollen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer sind nach vorheriger Anmeldung mit angemessener Frist (mindestens zwei Wochen) während der üblichen Geschäftszeiten des Auftragsverarbeiters möglich, sofern hierdurch keine unverhältnismäßigen Beeinträchtigungen des Geschäftsbetriebs des Auftragsverarbeiters oder Dritter entstehen. Der Auftragsverarbeiter kann die Kosten einer solchen Vor-Ort-Kontrolle dem Verantwortlichen in Rechnung stellen, soweit die Kontrolle mehr als einmal jährlich ohne Anlass erfolgt.

§ 10 Haftung

Für die Haftung der Parteien im Rahmen dieses AVV gelten die Haftungsregelungen des Hauptvertrags (insbesondere § 5 der Allgemeinen Geschäftsbedingungen der novendix GmbH) entsprechend, soweit zwingende Vorschriften der DSGVO (insbesondere Art. 82 DSGVO) nicht entgegenstehen. Die Pflichten des Auftragsverarbeiters aus diesem AVV sind wesentliche Vertragspflichten im Sinne von § 5.2 der AGB.

§ 11 Schlussbestimmungen

11.1 Änderungen und Ergänzungen dieses AVV bedürfen der Textform, soweit nicht in diesem AVV etwas anderes bestimmt ist (vgl. §§ 5.2 und 11.2).

11.2 Der Auftragsverarbeiter ist berechtigt, diesen AVV mit Wirkung für die Zukunft zu ändern, soweit die Änderung (a) aufgrund geänderter gesetzlicher Vorgaben, Rechtsprechung oder Anforderungen von Aufsichtsbehörden erforderlich ist, (b) technische oder organisatorische Änderungen der Plattform abbildet oder (c) der Klarstellung dient. Das Schutzniveau für die personenbezogenen Daten des Verantwortlichen darf dadurch nicht sinken; Einschränkungen der Pflichten des Auftragsverarbeiters nach Art. 28 Abs. 3 DSGVO sind auf diesem Weg ausgeschlossen. Der Auftragsverarbeiter teilt die Änderung mindestens vier (4) Wochen vor ihrem Inkrafttreten in Textform mit und stellt die geänderte Fassung zur Verfügung. Widerspricht der Verantwortliche nicht innerhalb von zwei (2) Wochen nach Zugang in Textform, gilt die Änderung als genehmigt; hierauf weist der Auftragsverarbeiter in der Mitteilung gesondert hin. Im Fall eines Widerspruchs gilt die bisherige Fassung fort.

11.3 Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

11.4 Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.