

Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 Abs. 3 DSGVO für die Nutzung der Plattform Norminator (norminator.de)

Stand: August 2026 · Revision 00

Der nachfolgende Vertrag regelt die Auftragsverarbeitung nach Art. 28 DSGVO für die Nutzung der SaaS-Plattform Norminator (norminator.de). Norminator ist ein KI-gestützter Assistent für Managementsysteme (Qualität, Umwelt, Arbeitsschutz, Informationssicherheit und weitere Normen) und erbringt keine Rechtsdienstleistungen im Sinne des Rechtsdienstleistungsgesetzes (RDG). Dieser Vertrag richtet sich an Auftraggeber, die Norminator als Unternehmen oder Organisation einsetzen.

Vertragsparteien

Auftraggeber (Verantwortlicher):

Auftragnehmer (Auftragsverarbeiter):

Privates Institut für Qualität und Innovation GmbH

Niedensteinsweg 8

59846 Sundern

Deutschland

Vertreten durch die Geschäftsführung: Leif vom Lehn, Paula vom Lehn

Telefon: 02933 786 3185

E-Mail: info@iqi-gmbh.de

Präambel

Der Auftraggeber nutzt die SaaS-Plattform Norminator (nachfolgend „Plattform“) des Auftragnehmers zur KI-gestützten Erstellung, Prüfung und Weiterentwicklung von Dokumenten und Inhalten seines Managementsystems (z. B. Auditberichte, FMEAs, Prozessbeschreibungen, Schulungsunterlagen), zur Recherche in Normen und Rechtsvorschriften sowie zur Beratung im Dialog. Kern der Plattform ist die Verarbeitung der Eingaben, Gesprächsverläufe und hochgeladenen Dokumente des Auftraggebers durch Sprachmodelle externer Anbieter (§ 10a, Anlage 4). Im Rahmen dieser Nutzung verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag regelt die Auftragsverarbeitung gemäß Art. 28 DSGVO.

§ 1 Gegenstand und Dauer der Verarbeitung

- (1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der Bereitstellung und Nutzung der Plattform Norminator gemäß den Bestimmungen des zwischen den Parteien geschlossenen Nutzungsvertrages (Abonnement nach den Allgemeinen Geschäftsbedingungen oder Unternehmensvereinbarung).
- (2) Die Verarbeitung erfolgt ausschließlich im Rahmen der Nutzung der Plattform als KI-gestützter Assistent für Managementsysteme.
- (3) Dieser Vertrag gilt für die Dauer des Nutzungsvertrages über die Plattform. Er endet automatisch mit Beendigung des Nutzungsvertrages, unbeschadet der Regelungen zur Löschung und Rückgabe in § 12.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Zweck der Verarbeitung ist die Bereitstellung der Plattform als webbasierter KI-Assistent für Managementsysteme, insbesondere:

- Beratung im Dialog: Beantwortung von Fragen und Bearbeitung von Aufgaben der Nutzer durch Sprachmodelle externer Anbieter (§ 10a, Anlage 4)
- Verarbeitung hochgeladener Dokumente (Text- und Office-Dateien, Bilder, gescannte Dokumente) als Grundlage der Beratung und Dokumenterstellung
- Erstellung von Dokumenten und Dateien in Office-, Web- und Lernformaten (Word, Excel, PowerPoint, PDF, HTML, SCORM u. a.)
- Projekte mit Projektkontext und Projektablage sowie – im Unternehmenstarif – gemeinsame Arbeitsbereiche mehrerer Nutzer
- Hilfsdienste zur Gesprächsführung: automatische Zusammenfassungen von Nachrichten, Gesprächsabriss, Erinnerungen, Gesprächstitel
- Web-Recherche des Assistenten über eine vom Auftragnehmer betriebene Metasuchmaschine und Abruf öffentlicher Webseiten (§ 10a Abs. 7)
- Recherche in der vom Auftragnehmer betriebenen Rechtskatalog-Datenbank (rechtskatalog.com) – kein Dritter beteiligt

- Werkstatt (nur nach gesonderter Freigabe): Zugriff des Assistenten auf vom Auftraggeber benannte Code-Ablagen bei dessen Anbieter mit einem vom Auftraggeber bereitgestellten Zugang
- Verwaltung von Nutzerkonten, Abonnements, Abrechnung und Support

(2) Die Verarbeitung erfolgt ausschließlich auf Weisung des Auftraggebers, soweit in diesem Vertrag oder im Nutzungsvertrag nicht anders geregelt.

(3) Der Umfang der Verarbeitung ergibt sich aus dem Nutzungsvertrag, den auf der Plattform verfügbaren Funktionen sowie den vom Auftraggeber und seinen Nutzern eingegebenen, hinterlegten und hochgeladenen Daten.

§ 3 Arten personenbezogener Daten und Kategorien betroffener Personen

(1) Die im Rahmen der Plattformnutzung verarbeiteten personenbezogenen Daten umfassen:

- Bestandsdaten: Vor- und Nachname, Anzeigename, E-Mail-Adresse, Unternehmen, Rolle/Berechtigung; bei kostenpflichtigen Abonnements zusätzlich Rechnungsadresse und Umsatzsteuer-Identifikationsnummer
- Anmeldedaten: E-Mail-Adresse, Passwort (ausschließlich gehasht), Sitzungs-Token
- Vertrags- und Zahlungsdaten: Abonnement, Laufzeit, Status, Kennungen des Zahlungs- und Rechnungsdienstleisters (keine Kartendaten beim Auftragnehmer)
- Inhaltsdaten: Eingaben der Nutzer im Dialog und die Antworten, Gesprächsverläufe, hochgeladene Dateien und erzeugte Dokumente, Projekte mit Projektkontext und Ablage, vom Nutzer hinterlegter persönlicher Kontext und Unternehmensangaben, vom System erzeugte Zusammenfassungen, Gesprächsabrisse und Erinnerungen
- Nutzungsdaten: Zeitpunkte, genutzte Funktionen, je Anfrage Anbieter, Dauer und Umfang (Token) der KI-Verarbeitung
- Server-Logfiles: IP-Adresse, Browsertyp/-version, Betriebssystem, Uhrzeit der Serveranfrage; Betriebsprotokolle der Anwendung mit Kennungen und kurzen Anfangsausschnitten von Nachrichten zur Störungsanalyse (rotierend gelöscht)
- Support-Anfragen: Kontaktdaten, Anliegen, technische Umgebung und ein Auszug der letzten Nachrichten des Nutzers, soweit der Nutzer eine Support-Anfrage aus der Anwendung stellt

(2) Kategorien betroffener Personen:

- Beschäftigte und sonstige Nutzer des Auftraggebers, denen ein Plattform-Zugang eingerichtet wurde
- Ansprechpartner des Auftraggebers für Vertrag, Abrechnung und Support
- Personen, die in den vom Auftraggeber eingegebenen Inhalten, hinterlegten Kontexten oder hochgeladenen Dokumenten genannt werden

(3) Hinweis zur Datenminimierung (Privacy by Design, Art. 25 DSGVO): Anzeigename, persönlicher Kontext, Projektkontext und Unternehmensangaben werden dem Sprachmodell bei jeder Anfrage mitgegeben (§ 10a Abs. 3). Der Auftraggeber kann diese Angaben neutral wählen (z. B. Funktionsbezeichnung statt Klarnamen) und hält seine Nutzer an, im persönlichen Kontext keine

vertraulichen oder personenbezogenen Angaben Dritter zu hinterlegen. Die Plattform unterstützt die Nutzung von Funktionspostfächern anstelle persönlicher E-Mail-Adressen.

(4) Datenminimierung vor dem Upload: Der Auftraggeber wählt die hochgeladenen Dokumente und die eingegebenen Inhalte eigenverantwortlich aus. Er wird vor dem Upload personenbezogene Daten, die für die Aufgabe nicht erforderlich sind, nach Möglichkeit entfernen oder unkenntlich machen, und Dokumente mit besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO nur hochladen, soweit deren Verarbeitung tatsächlich erforderlich ist. Der Auftragnehmer nimmt keine inhaltliche Vorauswahl und keine automatische Bereinigung der Inhalte vor (Art. 5 Abs. 1 lit. c, Art. 25 DSGVO).

§ 4 Weisungsrecht

- (1) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich auf Weisung des Auftraggebers, es sei denn, er ist durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- (2) Weisungen werden durch den Nutzungsvertrag, diesen Vertrag sowie durch die Konfiguration und Nutzung der Plattform durch den Auftraggeber und seine Nutzer erteilt (insbesondere durch Eingaben, Uploads, Projekt- und Kontexteinstellungen sowie Freigaben). Weisungen können auch durch die Einstellungen und Softwarefunktionalitäten der Plattform erteilt werden.
- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzbestimmungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 5 Pflichten des Auftragsverarbeiters

- (1) Der Auftragnehmer verarbeitet die ihm im Rahmen des Auftragsverhältnisses überlassenen personenbezogenen Daten nicht für eigene Zwecke. Insbesondere werden Inhalte des Auftraggebers weder vom Auftragnehmer noch – nach den vertraglichen Zusicherungen – von den in Anlage 4 genannten Anbietern zum Training von KI-Modellen verwendet. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt; ausgenommen sind die zur Verfügbarkeit erforderlichen Sicherungen (Anlage 1).
- (2) Der Auftragnehmer hält die einschlägigen datenschutzrechtlichen Vorschriften ein, insbesondere die DSGVO und das BDSG.
- (3) Der Auftragnehmer unterstützt den Auftraggeber bei der Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO, indem er die erforderlichen Informationen über die im Rahmen der Plattform durchgeführten Verarbeitungstätigkeiten bereitstellt (Anlage 3, Anlage 4).

§ 6 Verschwiegenheitspflicht

(1) Der Auftragnehmer stellt sicher, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Verschwiegenheit verpflichtet sind, soweit sie keiner gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Die Verschwiegenheitspflicht besteht über das Ende des Beschäftigungsverhältnisses bzw. der Beauftragung hinaus.

§ 7 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragnehmer ergreift alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Maßnahmen sind in Anlage 1 (TOM) dieses Vertrages beschrieben.

(2) Die Maßnahmen umfassen insbesondere:

- Durchgehende TLS-Verschlüsselung der Datenübertragung – auch zu den Anbietern der KI-Verarbeitung
- Mandantentrennung: jede Datenbankabfrage ist serverseitig an die Organisationskennung aus dem signierten Sitzungs-Token gebunden
- Signierte Sitzungs-Token in HttpOnly-, Secure- und SameSite-geschützten Cookies; Passwörter ausschließlich gehasht
- Hosting, Datenbanken und Sicherungen ausschließlich in der EU (Rechenzentrumsregion Frankfurt am Main)
- Datenbanken und Hilfsdienste nur im internen Netz des Servers erreichbar; Werkzeuge des Assistenten in isolierten Containern
- Kein Tracking und keine Werbe-Cookies in der Anwendung; ausschließlich technisch nötige Cookies
- Maskierung von Zugangsschlüsseln in Protokollen; rotierende Löschung der Protokolle

(3) Der Auftragnehmer passt die Maßnahmen der technischen und organisatorischen Weiterentwicklung an und informiert den Auftraggeber über wesentliche Änderungen.

(4) Für Auftraggeber, die ein ISMS nach ISO/IEC 27001 betreiben, über TISAX zertifiziert sind oder BSI-GV-Vorgaben zu beachten haben: Die TOM des Auftragnehmers sind so ausgestaltet, dass sie den Anforderungen an die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO in Verbindung mit den jeweiligen normativen Anforderungen (ISO/IEC 27001 Annex A, BSI IT-Grundschutz, TISAX-Assessment-Kriterien) gerecht werden. Die in Anlage 1 dokumentierten Maßnahmen können als Nachweis im Rahmen von Audits und Assessment-Ergebnissen herangezogen werden.

(5) Einzelheiten zu Schlüsselmanagement, Sicherungsverschlüsselung, Löschkonzept produktiver Systeme, Wiederherstellungszeiten (RTO/RPO) und Prüfturnus stellt der Auftragnehmer dem Auftraggeber und dessen Datenschutzbeauftragtem auf Anforderung in einem nicht-öffentlichen, versionierten TOM-Detailldokument gegen Vertraulichkeitsvereinbarung zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO).

§ 8 Unterstützung des Verantwortlichen

- (1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen auf Wahrung der Rechte betroffener Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 lit. e DSGVO). Nutzer können Gespräche, Dateien, Projekte und Erinnerungen in der Anwendung selbst löschen; Auskunfts- und Löschersuchen, die darüber hinausgehen, erfüllt der Auftragnehmer auf Anforderung des Auftraggebers.
- (2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Durchführung von Datenschutz-Folgenabschätzungen, soweit diese die spezifische Verarbeitung auf der Plattform betreffen (Art. 28 Abs. 3 lit. f DSGVO).
- (3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, leitet der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiter.

§ 9 Meldepflicht bei Datenschutzverletzungen

- (1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.
- (2) Die Meldung erfolgt unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, um dem Auftraggeber die Einhaltung seiner Meldefristen nach Art. 33 und Art. 34 DSGVO zu ermöglichen.
- (3) Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei der Meldung an die zuständige Aufsichtsbehörde (Art. 33 DSGVO) und der Benachrichtigung betroffener Personen (Art. 34 DSGVO).
- (4) Die Meldung enthält mindestens: Art der Verletzung, Art und Umfang der betroffenen personenbezogenen Daten, Zeitpunkt der Feststellung, wahrscheinliche Folgen, Maßnahmen zur Behebung und Schadensbegrenzung.

§ 10 Subunternehmer / Weitere Auftragsverarbeiter

- (1) Der Auftragnehmer setzt zur Erfüllung des Nutzungsvertrages folgende weitere Auftragsverarbeiter ein. Eine detaillierte Übersicht befindet sich in Anlage 2. Die Anbieter der KI-Verarbeitung (Sprachmodelle und multimodale Modelle) sind in Anlage 4 aufgeführt; ihre Einbindung regelt § 10a.

Dienstleister	Sitz	Zweck	Drittland
Amazon Web Services EMEA SARL	Luxemburg (EU); Verarbeitung in der Rechenzentrumsregion Frankfurt am Main (Deutschland)	Hosting der Plattform, Datenbanken und Sicherungen	Nein

Dienstleister	Sitz	Zweck	Drittland
Anbieter der KI-Verarbeitung nach Anlage 4 (acht Anbieter)	USA, Frankreich, Vereinigtes Königreich	Betrieb der Sprachmodelle und multimodalen Modelle (§ 10a)	Ja (außer Mistral AI); Einzelheiten Anlage 4
Stripe Payments Europe, Limited	Irland (EU)	Zahlungsabwicklung (nur bei Abschluss eines Abonnements über die Plattform)	Nein
easybill GmbH	Deutschland (EU)	Rechnungserstellung und -versand (nur nach Vertragsabschluss)	Nein
Zapier, Inc.	USA	Technische Automatisierung: Übergabe von Vertragseignissen an die Kundenverwaltung, Support-Anfragen aus der Anwendung, Anfragen zum Unternehmenstarif	Ja
Marketcircle Inc.	Kanada	Kunden- und Vertragsverwaltung/CRM (nur nach Vertragsabschluss)	Ja
Microsoft Ireland Operations Limited	Irland (EU)	Versand von Transaktions-E-Mails (Registrierung, Passwort, Kontohinweise)	Nein

(2) Mit allen Dienstleistern bestehen Auftragsverarbeitungsverträge nach Art. 28 DSGVO.

(3) Für Dienstleister mit Sitz außerhalb der EU werden EU-Standardvertragsklauseln nach Art. 46 DSGVO nebst ergänzenden Schutzmaßnahmen vereinbart; soweit ein Anbieter zusätzlich nach dem EU-US Data Privacy Framework zertifiziert ist (Zapier), stützt sich die Übermittlung auch auf den Angemessenheitsbeschluss der EU-Kommission. Für Marketcircle (Kanada) besteht ein Angemessenheitsbeschluss der EU-Kommission (PIPEDA). Der Hosting-Anbieter verarbeitet die Daten ausschließlich in Rechenzentren in Deutschland (Region Frankfurt am Main); für etwaige Fernzugriffe des Hosting-Anbieters aus Drittländern im Rahmen von Betrieb und Support gelten die in dessen Datenverarbeitungszusatz vereinbarten EU-Standardvertragsklauseln. Für die Anbieter der KI-Verarbeitung gilt § 10a in Verbindung mit Anlage 4.

(4) Die KI-Modelle werden nicht mit Inhalten des Auftraggebers trainiert (§ 5 Abs. 1, Anlage 4 Abschnitt D).

(5) Der Auftragnehmer informiert den Auftraggeber in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters — einschließlich der Anbieter nach Anlage 4 —, und zwar mindestens vier Wochen vor deren Wirksamwerden, unter Angabe von Name, Sitz und Verarbeitungszweck. Der Auftraggeber kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus einem datenschutzrechtlich begründeten Grund in Textform widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Änderung als genehmigt.

(6) Widerspricht der Auftraggeber, teilt der Auftragnehmer ihm innerhalb von 14 Tagen nach Zugang des Widerspruchs in Textform mit, ob er von der Änderung absieht, sie für den Auftraggeber nicht anwendet oder eine gleichwertige Lösung anbietet. Kommt innerhalb von 30 Tagen nach Zugang des Widerspruchs keine Einigung zustande, ist der Auftraggeber berechtigt, diesen Vertrag und den Nutzungsvertrag außerordentlich mit Wirkung zum Zeitpunkt des Wirksamwerdens der Änderung zu kündigen. Im Voraus entrichtete Entgelte für den nicht mehr in Anspruch genommenen Leistungszeitraum werden anteilig erstattet.

§ 10a KI-Verarbeitung durch Sprachmodelle externer Anbieter

(1) Gegenstand: Die Beratung im Dialog, die Verarbeitung hochgeladener Dokumente, die Erstellung von Dokumenten sowie die Hilfsdienste nach § 2 Abs. 1 werden durch Sprachmodelle und multimodale Modelle erbracht, die von den in Anlage 4 genannten Anbietern betrieben werden. Diese Verarbeitung ist Kern der Plattform; sie erfolgt bei jeder Nutzung und nicht erst nach gesonderter Buchung. Mit Abschluss des Nutzungsvertrages weist der Auftraggeber den Auftragnehmer an, diese Verarbeitung durchzuführen (§ 4); er bestätigt, die Angaben zur Drittlandübermittlung in Anlage 4 zur Kenntnis genommen zu haben.

(2) Verarbeitungsketten: Für jeden Zweck ist in Anlage 4 Abschnitt A eine feste Reihenfolge von Anbietern hinterlegt. Eine Anfrage wird an den ersten Anbieter der jeweiligen Kette gerichtet; steht dieser nicht zur Verfügung oder antwortet er nicht brauchbar, wird der nächste Anbieter derselben Kette genutzt. Anbieter außerhalb der hinterlegten Ketten werden nicht angesprochen; im Programmcode der Plattform sind keine weiteren Anbieter eingebunden.

(3) Datenumfang: Je Anfrage übermittelt der Auftragnehmer an den jeweils genutzten Anbieter die Eingabe des Nutzers und den Verlauf des Gesprächs (bzw. dessen Abriss), die Inhalte der in diesem Gespräch oder Projekt hochgeladenen Dateien im Volltext einschließlich Dateinamen, den Anzeigenamen des Nutzers, die Unternehmensbezeichnung, den vom Nutzer hinterlegten persönlichen Kontext, den Projektkontext, ausgewählte Erinnerungen sowie Gestaltungsangaben des Unternehmenstarifs. Hochgeladene Bilder und gescannte Dokumentseiten werden als Bilddaten zusammen mit einem Ausschnitt der Anfrage an die multimodalen Modelle übermittelt. Der Zusammenfassungsdienst erhält jede Nachricht und jede Antwort einschließlich der enthaltenen Dateitexte in gekürzter Form. Nicht übermittelt werden E-Mail-Adressen, Passwörter, Zahlungs- und Rechnungsdaten, Daten anderer Organisationen sowie Inhalte gelöschter Gespräche. Eine automatische Anonymisierung findet nicht statt; welche personenbezogenen Daten enthalten sind, bestimmt der Auftraggeber durch seine Eingaben, Uploads und Profilangaben (§ 3 Abs. 3 und 4). Die Einzelheiten beschreibt Anlage 4 Abschnitt B.

(4) Drittlandübermittlung: Mit Ausnahme des Anbieters mit Sitz in der EU (Mistral AI) haben die Anbieter ihren Sitz in den USA bzw. im Vereinigten Königreich. Die Übermittlung erfolgt auf Grundlage der mit dem jeweiligen Anbieter vereinbarten EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO), für das Vereinigte Königreich zusätzlich auf Grundlage des Angemessenheitsbeschlusses der EU-Kommission, nebst den in Anlage 4 Abschnitt D beschriebenen ergänzenden Maßnahmen. Die übermittelten Inhalte werden von keinem Anbieter zum Training von KI-Modellen verwendet; soweit

ein Anbieter eine Betriebsart ohne Speicherung der Eingaben und Ausgaben anbietet, nutzt der Auftragnehmer diese.

(5) Speicherung und Löschung beim Auftragnehmer: Gespräche, hochgeladene Dateien, erzeugte Dokumente, Projekte, Erinnerungen, Zusammenfassungen und Gesprächsabrisse werden beim Auftragnehmer gespeichert, damit der Nutzer sie weiterverwenden kann. Sie bleiben gespeichert, bis der Nutzer oder der Auftraggeber sie löscht oder der Nutzungsvertrag endet (§ 12). Vom Nutzer gelöschte Gespräche und Dateien werden 30 Tage nach der Löschung endgültig entfernt. Je Anfrage protokolliert der Auftragnehmer Zeitpunkt, Benutzer- und Organisationskennung, Anbieter, Modell, Dauer und Umfang (Token) für Abrechnung und Störungsanalyse.

(6) Pflichten des Auftraggebers: Der Auftraggeber weist seine Nutzer an, in Eingaben, Kontexten und Uploads keine personenbezogenen Daten Dritter zu verwenden, die für die Aufgabe nicht erforderlich sind, und besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) nur zu verarbeiten, soweit dies tatsächlich erforderlich ist. Er stellt sicher, dass für die von ihm hochgeladenen Inhalte eine Rechtsgrundlage besteht.

(7) Web-Recherche: Recherchiert der Assistent im Internet, übermittelt der Auftragnehmer die vom Sprachmodell aus der Anfrage gebildeten Suchbegriffe über eine selbst betriebene Metasuchmaschine an öffentliche Suchmaschinen und ruft öffentlich zugängliche Webseiten ab. Die Suchbegriffe können Inhalte aus der Anfrage des Nutzers enthalten. Die Betreiber der Suchmaschinen und der abgerufenen Webseiten sind keine Auftragsverarbeiter des Auftragnehmers; sie erhalten keine Kennung des Nutzers oder des Auftraggebers. Der Auftraggeber weist seine Nutzer an, keine personenbezogenen Daten in Anfragen aufzunehmen, die eine Web-Recherche auslösen sollen.

(8) Die Ergebnisse der KI-Verarbeitung sind Vorschläge und Entwürfe, die der Auftraggeber vor ihrer Verwendung prüft. Sie sind keine Rechtsberatung im Sinne des Rechtsdienstleistungsgesetzes (RDG).

§ 11 Kontrollrechte und Audit

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung.

(2) Der Auftragnehmer ermöglicht dem Auftraggeber nach entsprechender Terminvereinbarung Überprüfungen einschließlich Inspektionen, die vom Auftraggeber oder einem von ihm beauftragten Prüfer durchgeführt werden.

(3) Für Auftraggeber mit ISMS nach ISO/IEC 27001, TISAX-Assessment oder BSIG-Konformität: Die Überprüfung kann im Rahmen der internen Audits, TISAX-Assessment-Prozesse oder BSI-Konformitätsprüfungen des Auftraggebers erfolgen. Der Auftragnehmer unterstützt diese Prüfungen durch Bereitstellung relevanter Dokumentation (TOM, Subunternehmer-Verzeichnis, Vereinbarungen mit den Anbietern nach Anlage 4, Sicherheitskonzepte).

(4) Soweit der Auftragnehmer durch eine anerkannte Zertifizierung oder ein genehmigtes Zertifizierungsverfahren nach Art. 42 DSGVO nachweist, dass er die erforderlichen Maßnahmen getroffen hat, kann dies als Faktor für den Nachweis herangezogen werden. Eine zwingende Vor-Ort-Kontrolle ist dann nicht erforderlich.

§ 12 Löschung und Rückgabe

- (1) Nutzer können Gespräche, Dateien, Projekte und Erinnerungen jederzeit in der Anwendung löschen; gelöschte Inhalte werden 30 Tage nach der Löschung endgültig entfernt. Erzeugte Dokumente stehen den Nutzern als Download zur Verfügung.
- (2) Nach Beendigung des Nutzungsvertrages löscht der Auftragnehmer die Nutzerkonten und alle Inhalte des Auftraggebers auf dessen Anforderung, spätestens jedoch 90 Tage nach Beendigung, sofern der Auftraggeber nicht vorher die Rückgabe in einem gängigen Format verlangt.
- (3) Die Löschung ist dem Auftraggeber auf Verlangen mit Datumsangabe in Textform zu bestätigen.
- (4) Sicherungen werden spätestens 30 Tage nach der Löschung der Daten überschrieben bzw. gelöscht.
- (5) Soweit gesetzliche Aufbewahrungspflichten bestehen (insbesondere für Rechnungs- und Vertragsdaten), kann der Auftragnehmer die Daten bis zum Ablauf der Aufbewahrungsfrist speichern, verpflichtet sich jedoch, diese Daten ausschließlich zur Erfüllung der gesetzlichen Pflichten zu verarbeiten.

§ 13 Haftung

- (1) Die Haftung der Parteien richtet sich nach den Bestimmungen der DSGVO, insbesondere Art. 82 DSGVO, sowie den gesetzlichen Vorschriften.
- (2) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die er durch nicht vorschriftsmäßige Verarbeitung verursacht hat, soweit er seinen Pflichten nach Art. 28 DSGVO nicht nachgekommen ist.

§ 14 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Aufhebung der Schriftform.
- (2) Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein, so bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.
- (3) Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland.
- (4) Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.
- (5) Anlagen sind Bestandteil dieses Vertrages: Anlage 1 (TOM), Anlage 2 (Subunternehmer-Verzeichnis), Anlage 3 (Beschreibung der Verarbeitungstätigkeit), Anlage 4 (KI-Verarbeitung: Verarbeitungsketten, Datenumfang und Anbieter).

Unterschriften

Dieser Auftragsverarbeitungsvertrag bedarf gemäß Art. 28 Abs. 9 DSGVO der Textform; eine handschriftliche Unterschrift ist nicht erforderlich. Mit dem Ausfüllen der Vertragsdaten und der Rücksendung an IQI (z. B. per E-Mail an info@iqi-gmbh.de) gilt der Vertrag als abgeschlossen.

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

Maßnahmen-Bereich	Konkrete Maßnahmen
1. Zutrittskontrolle (physischer Zugang zu Räumen)	Hosting bei Amazon Web Services in der Rechenzentrumsregion Frankfurt am Main (Deutschland): Rechenzentren mit Zutrittskontrolle, Videoüberwachung und Zugang nur für autorisiertes Personal; zertifiziert u. a. nach ISO/IEC 27001 und SOC 1/2/3
2. Zugangskontrolle (logischer Zugang zu Systemen)	Personalisierte Benutzerkonten mit Rollen (Inhaber, Administrator, Mitglied); Passwörter ausschließlich gehasht (bcrypt); signierte Sitzungs-Token in HttpOnly-, Secure- und SameSite-Cookies mit kurzer Laufzeit und serverseitiger Sperrliste; Administrationszugänge zum Server nur über geschützte, personengebundene Verbindungen; Verwaltungsoberfläche des Auftragnehmers getrennt von der Anwendung
3. Zugriffskontrolle (Zugriff auf Daten)	Mandantentrennung: die Organisationskennung wird serverseitig aus dem signierten Token gebildet, nie aus der Anfrage; Datenbanken, Zwischenspeicher, Suchdienst und Vektorspeicher sind nur im internen Netz des Servers erreichbar; Werkzeuge des Assistenten laufen in isolierten Containern (Sandbox nur lesend, eigenes Netz); Zugangsschlüssel zu den Anbietern liegen ausschließlich serverseitig
4. Datenträgerkontrolle	Verschlüsselte Datenträger des Hosting-Anbieters; Sicherungen auf dem Server des Auftragnehmers mit begrenzter Vorhaltezeit (7 Tage); physische Schutzmaßnahmen im Rechenzentrum
5. Übertragungskontrolle	Durchgehende TLS-Verschlüsselung aller Datenübertragungen – Browser, Schnittstellen und Anbieter der KI-Verarbeitung; signierte Sitzungs-Token; keine unverschlüsselte Übertragung personenbezogener Daten
6. Eingabekontrolle	Zeitstempel und Urheber an Gesprächen, Dateien, Projekten und Erinnerungen; Protokollierung je KI-Anfrage (Zeitpunkt, Kennungen, Anbieter, Dauer); Nachvollziehbarkeit von Änderungen an Konten und Abonnements
7. Verfügbarkeitskontrolle	Regelmäßige Sicherungen der Datenbanken (Vorhaltezeit 7 Tage), Zustandsprüfungen der Dienste mit automatischem Neustart, Überwachung der Erreichbarkeit mit Alarmierung, Ausweichketten bei Ausfall eines Anbieters der KI-Verarbeitung, Notfallkonzept
8. Trennungskontrolle	Strikte Trennung der Organisationen; Trennung der Anwendung vom öffentlichen Webauftritt; Trennung der Wissensbasis (Normen, Fachinhalte) vom Kundenbestand; Entwicklung und Test getrennt von der Produktion (Versionsverwaltung, Testsuite vor jeder Einspielung)
9. Pseudonymisierung und Datenminimierung	Anzeigenname, persönlicher Kontext und Unternehmensangaben frei wählbar (Funktionsbezeichnungen möglich); E-Mail-Adressen, Zahlungs- und Rechnungsdaten werden nicht an die Anbieter der KI-Verarbeitung übermittelt; Hinweis zur Datenminimierung beim Upload; Unterstützung von Funktionspostfächern

Maßnahmen-Bereich	Konkrete Maßnahmen
10. Verschlüsselung	TLS-Verschlüsselung der Datenübertragung, Passwort-Hashing (bcrypt), Signatur der Sitzungs-Token, verschlüsselte Datenträger
11. Verfahrensweisen	Maskierung von Zugangsschlüsseln in allen Protokollen; rotierende Löschung der Protokolle; Änderungen am Programmcode über Versionsverwaltung mit automatischen Tests; Incident-Response-Prozess; dokumentierte Betriebsabläufe
12. Datenschutz durch Technikgestaltung	Kein Tracking und keine Werbe-Cookies in der Anwendung; Web-Analyse des öffentlichen Webauftritts nur cookielos und auf eigenen Servern; kein Training von KI-Modellen mit Kundendaten (vertraglich mit jedem Anbieter); Betriebsart ohne Speicherung bei den Anbietern, soweit angeboten; feste Anbieterketten ohne Ausweichen auf nicht benannte Anbieter
13. Informationssicherheitsmanagement	TOM ausgerichtet an den Anforderungen der ISO/IEC 27001 Annex A, BSI IT-Grundschutz und TISAX-Assessment-Kriterien; Maßnahmen können als Nachweis im Rahmen von Audits herangezogen werden; Detailangaben nach § 7 Abs. 5 im nicht-öffentlichen TOM-Detaildokument

Anlage 2 – Verzeichnis der Subunternehmer

Dienstleister	Sitz	Zweck der Verarbeitung	Drittland-Schutzmaßnahme	Art der Daten
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	Luxemburg (EU); Verarbeitung in der Rechenzentrumsregion Frankfurt am Main (Deutschland)	Hosting der Plattform, Datenbanken, Sicherungen, Server-Logfiles	Nicht erforderlich (Verarbeitung in der EU); für etwaige Fernzugriffe des Anbieters aus Drittländern gelten die EU-Standardvertragsklauseln des AWS-Datenverarbeitungszusatzes	Alle Plattform-Daten nach § 3
Anbieter der KI-Verarbeitung (Anlage 4 C, Nr. 1–8)	USA; Frankreich (EU); Vereinigtes Königreich	Betrieb der Sprachmodelle und multimodalen Modelle für Dialog, Dokumenterstellung, Hilfsdienste, Zusammenfassungen, Bilder und Scans	EU-Standardvertragsklauseln je Anbieter; Vereinigtes Königreich: Angemessenheitsbeschluss; Mistral AI: nicht erforderlich (EU); ergänzende Maßnahmen Anlage 4 D	Eingaben, Gesprächsverläufe, Dateihalte, Bilder, Kontexte nach Anlage 4 B

Dienstleister	Sitz	Zweck der Verarbeitung	Drittland-Schutzmaßnahme	Art der Daten
Stripe Payments Europe, Limited, One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Irland	Irland (EU)	Zahlungsabwicklung für Abonnements, Kundenportal	Nicht erforderlich (EU); für Verarbeitungen durch Stripe-Gesellschaften in den USA gelten die EU-Standardvertragsklauseln und das EU-US Data Privacy Framework nach dem Stripe-Datenverarbeitungszusatz	Name, E-Mail-Adresse, Rechnungsadresse, USt-IdNr., Zahlungsdaten (nur bei Abonnement über die Plattform)
easybill GmbH, Düsselstraße 21, 41564 Kaarst	Deutschland (EU)	Erstellung und Versand von Rechnungen	Nicht erforderlich (EU)	Name, Unternehmen, E-Mail-Adresse, Rechnungsadresse, USt-IdNr., Rechnungsbeträge (nur nach Vertragsabschluss)
Zapier, Inc., 548 Market Street #62411, San Francisco, CA 94104, USA	USA	Technische Automatisierung: Übergabe von Vertragsereignissen (Abschluss, Verlängerung, Kündigung) an die Kundenverwaltung; Support-Anfragen aus der Anwendung; Anfragen zum Unternehmenstarif	EU-US Data Privacy Framework (Zertifizierung des Anbieters) und EU-Standardvertragsklauseln (Art. 46 DSGVO) gemäß Datenverarbeitungszusatz des Anbieters	Name, E-Mail-Adresse, Unternehmen, USt-IdNr., Abonnementdaten; bei Support-Anfragen zusätzlich Rolle, Browser und ein Auszug der letzten drei Nachrichten des Nutzers
Marketcircle Inc., 30 Centurian Drive, Suite 201, Markham, ON L3R 8B8, Kanada	Kanada	Kunden- und Vertragsverwaltung (CRM Daylite)	Angemessenheitsbeschluss EU-Kommission (PIPEDA); Datenverarbeitungsvereinbarung des Anbieters	Kundenstammdaten, Vertragsdaten (nur nach Vertragsabschluss)

Dienstleister	Sitz	Zweck der Verarbeitung	Drittland-Schutzmaßnahme	Art der Daten
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Irland (EU)	Versand von Transaktions-E-Mails (Bestätigung der Registrierung, Passwort-Zurücksetzung, Kontohinweise)	Nicht erforderlich (EU); für etwaige Übermittlungen innerhalb des Microsoft-Konzerns gelten die EU-Standardvertragsklauseln des Microsoft-Datenschutznachtrags und das EU-US Data Privacy Framework	E-Mail-Adresse, Anzeigenname, Inhalt der Transaktionsmail

Die Dienstleister Stripe, easybill und Marketcircle werden erst mit Zustandekommen eines kostenpflichtigen Vertragsverhältnisses tätig. Die Anbieter der KI-Verarbeitung sind in Anlage 4 mit Anschrift, Zweck, Schutzmaßnahme und verbindlichen Unterlagen aufgeführt.

Anlage 3 – Beschreibung der Verarbeitungstätigkeit

Kriterium	Beschreibung
1. Verantwortlicher	[Auftraggeber – vom Kunden auszufüllen]
2. Auftragsverarbeiter	Privates Institut für Qualität und Innovation GmbH, Sundern
3. Gegenstand der Verarbeitung	Bereitstellung und Nutzung der SaaS-Plattform Norminator als KI-gestützter Assistent für Managementsysteme
4. Dauer der Verarbeitung	Dauer des Nutzungsvertrages
5. Art der Verarbeitung	Erhebung, Erfassung, Organisation, Ordnung, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung (an die Anbieter der KI-Verarbeitung), Verknüpfung, Einschränkung, Löschung, Vernichtung
6. Zweck der Verarbeitung	Beratung im Dialog, Verarbeitung hochgeladener Dokumente, Erstellung von Dokumenten, Projekte und gemeinsame Arbeitsbereiche, Hilfsdienste (Zusammenfassungen, Abrisse, Erinnerungen), Web- und Normenrecherche, Konto-, Vertrags- und Supportverwaltung
7. Art personenbezogener Daten	Bestandsdaten (Name, Anzeigenname, E-Mail-Adresse, Unternehmen, Rolle, Rechnungsadresse, USt-IdNr.), Anmeldedaten (gehashte Passwörter, Sitzungs-Token), Vertrags- und Zahlungsdaten (Abonnement, Dienstleisterkennungen), Inhaltsdaten (Eingaben, Antworten, Verläufe, Dateien, Projekte, Kontexte, Erinnerungen, Zusammenfassungen), Nutzungsdaten, Server-Logfiles, Support-Anfragen
8. Kategorien betroffener Personen	Beschäftigte und sonstige Nutzer des Auftraggebers mit Plattform-Zugang; Ansprechpartner für Vertrag, Abrechnung und Support; in Inhalten, Kontexten und Dokumenten genannte Personen

Kriterium	Beschreibung
9. Übermittlungen in Drittländer	KI-Verarbeitung durch Anbieter in den USA und im Vereinigten Königreich auf Grundlage von EU-Standardvertragsklauseln bzw. Angemessenheitsbeschluss (§ 10a, Anlage 4); Zapier (USA) auf Grundlage von EU-US Data Privacy Framework und EU-Standardvertragsklauseln; Marketcircle (Kanada) auf Grundlage des Angemessenheitsbeschlusses; Hosting ausschließlich in der EU
10. Technische und organisatorische Maßnahmen	Siehe Anlage 1
11. Datenschutzbeauftragter des Auftragsverarbeiters	Klaus Meissner, datenschutz@iqi-gmbh.de
12. Zuständige Aufsichtsbehörde	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW), Kavalleriestraße 2-4, 40213 Düsseldorf

Anlage 4 – KI-Verarbeitung: Verarbeitungsketten, Datenumfang und Unterauftragsverarbeiter

Diese Anlage beschreibt die Verarbeitung nach § 10a. Sie gilt für jede Nutzung der Plattform. Modellbezeichnungen werden nicht genannt; maßgeblich sind die Anbieter, die Reihenfolge und die vertraglichen Zusicherungen.

A. Verarbeitungsketten je Zweck

Zweck	Anbieterkette (in dieser Reihenfolge; der nächste nur bei Ausfall oder unbrauchbarer Antwort)
Beratung im Dialog: Antworten an den Nutzer, Werkzeugschritte des Assistenten (Recherche, Dateiverarbeitung, Dokumenterstellung im Gespräch)	1 Fireworks.ai → 2 Baseten → 3 Together → 4 Deep Infra → 5 OpenRouter
Dokumenterstellung und Hilfsdienste: Erzeugung von Office-, Web- und Lernformaten, Auswahl passender Erinnerungen, Gesprächsabriss, Gesprächstitel, Zusammenfassung des Denkverlaufs, Zusammenfassung jeder Nachricht und jeder Antwort (Kurzfassung für Verlauf und Suche)	1 Baseten → 2 Deep Infra → 3 Fireworks.ai → 4 Together → 5 OpenRouter
Reparatur fehlerhaft erzeugter Dateien	1 Baseten → 2 Deep Infra → 3 Fireworks.ai → 4 Together → 5 OpenRouter → 6 Cerebras → 7 Fireworks.ai (andere Modellklasse als letzte Reserve)
Bilder und gescannte Dokumentseiten (Beschreibung, Transkription)	1 Mistral AI (EU) → 2 Groq → 3 Deep Infra → 4 Deep Infra (zweites Modell)

OpenRouter ist eine Vermittlungsplattform: Sie leitet die Anfrage an einen von ihr eingesetzten Inferenz-Anbieter weiter. Der Auftragnehmer beschränkt diese Weiterleitung durch die Routing-Einstellung auf Anbieter, die Eingaben weder speichern noch zum Training verwenden; OpenRouter selbst speichert Eingaben und Ausgaben nicht (Unterlagen in Abschnitt C).

B. Übermittelte Daten je Anfrage

Übermittelt an den jeweils genutzten Anbieter	Nicht übermittelt
Die Eingabe des Nutzers und der Verlauf des Gesprächs bzw. dessen Abriss; die Inhalte der im Gespräch oder Projekt hochgeladenen Dateien im Volltext (Text-, Office- und PDF-Dateien) einschließlich Dateinamen; vom Assistenten erzeugte Dateien.	E-Mail-Adressen, Passwörter, Sitzungs-Token
Angaben aus dem Konto und dem Projekt: Anzeigenname des Nutzers, Unternehmensbezeichnung, vom Nutzer hinterlegter persönlicher Kontext, Projektkontext, bis zu fünf ausgewählte Erinnerungen, Gestaltungsangaben des Unternehmenstarifs (z. B. Farben).	Zahlungs- und Rechnungsdaten, USt-IdNr., Abonnementdaten
Bilder und gescannte Dokumentseiten als Bilddaten zusammen mit einem Ausschnitt der Anfrage (Kette „Bilder und Scans“).	Inhalte anderer Gespräche und Projekte, soweit sie nicht als Erinnerung oder Projektdatei ausgewählt sind
Für den Zusammenfassungsdienst: jede Nachricht und jede Antwort einschließlich der enthaltenen Dateitexte in gekürzter Form.	Daten anderer Organisationen; Inhalte gelöschter Gespräche

Eine automatische Anonymisierung findet nicht statt. Welche personenbezogenen Daten in den übermittelten Inhalten enthalten sind, bestimmt der Auftraggeber durch Eingaben, Uploads und Profilangaben; die Anwendung weist beim Upload auf die Datenminimierung hin (§ 3 Abs. 3 und 4, § 10a Abs. 6).

C. Unterauftragsverarbeiter der KI-Verarbeitung

Die Anfragen werden an die folgenden Anbieter in der in Abschnitt A angegebenen Reihenfolge gerichtet. Grundlage der Übermittlung in Drittländer sind die mit dem jeweiligen Anbieter vereinbarten EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO), für das Vereinigte Königreich der Angemessenheitsbeschluss der EU-Kommission, jeweils mit den ergänzenden Maßnahmen nach Abschnitt D. Die verbindlichen Unterlagen der Anbieter sind verlinkt; nicht öffentliche Vereinbarungen legt der Auftragnehmer dem Auftraggeber auf Verlangen vor.

Nr.	Anbieter	Sitz	Zweck (Kette und Position)	Drittland-Schutzmaßnahme	Verbindliche Unterlagen
1	Fireworks.ai, Inc. 2317 Broadway, Suite 200, Redwood City, CA 94063, USA	USA	Dialog-Sprachmodell (erster Anbieter der Kette); Sprachmodell für Dokumenterstellung, Hilfsdienste und Zusammenfassungen (dritter Anbieter); Reparatur (dritter und als letzte Reserve siebter Anbieter)	EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) gemäß Data Processing Addendum des Anbieters; ergänzende Maßnahmen nach Abschnitt D	Data Processing Addendum Datenschutzerklärung Datenumgang (keine Speicherung von Eingaben und Ausgaben) Trust Center (Zertifikate, Unterauftragsverarbeiter)
2	Baseten Labs, Inc. 201 Spear Street, Suite 1600, San Francisco, CA 94105, USA	USA	Dialog-Sprachmodell (zweiter Anbieter); Sprachmodell für Dokumenterstellung, Hilfsdienste, Zusammenfassungen und Reparatur (erster Anbieter)	EU-Standardvertragsklauseln gemäß Data Processing Addendum (Anlage II der Nutzungsbedingungen); ergänzende Maßnahmen nach Abschnitt D	Nutzungsbedingungen mit Data Processing Addendum Datenschutzerklärung Trust Center
3	Together Computer, Inc. 251 Rhode Island Street, Suite 200, San Francisco, CA 94103, USA	USA	Dialog-Sprachmodell (dritter Anbieter); Sprachmodell für Dokumenterstellung, Hilfsdienste, Zusammenfassungen und Reparatur (vierter Anbieter)	EU-Standardvertragsklauseln gemäß Data Processing Addendum des Anbieters (nicht öffentlich; wird dem Auftraggeber auf Verlangen vorgelegt); Betriebsart ohne Speicherung der Eingaben; ergänzende Maßnahmen nach Abschnitt D	Datenschutzerklärung Datenschutz und Sicherheit der Schnittstelle (keine Speicherung, kein Training) Trust Center

Nr.	Anbieter	Sitz	Zweck (Kette und Position)	Drittland-Schutzmaßnahme	Verbindliche Unterlagen
4	Deep Infra Inc. 2625 Middlefield Road #460, Palo Alto, CA 94306, USA	USA	Dialog-Sprachmodell (vierter Anbieter); Sprachmodell für Dokumenterstellung, Hilfsdienste, Zusammenfassungen und Reparatur (zweiter Anbieter); multimodales Modell für Bilder und Scans (dritter und vierter Anbieter)	EU-Standardvertragsklauseln gemäß Data Processing Addendum des Anbieters (nicht öffentlich; wird dem Auftraggeber auf Verlangen vorgelegt); keine Speicherung von Eingaben und Ausgaben nach den Nutzungsbedingungen; ergänzende Maßnahmen nach Abschnitt D	Nutzungsbedingungen Datenschutzerklärung Datenumgang der Schnittstelle Unterauftragsverarbeiter
5	OpenRouter, Inc. Gesellschaft nach dem Recht von Delaware, USA (Anschrift nach Registereintrag: 135 Greene Street, New York, NY 10012, USA)	USA	Vermittlungsplattform (fünfter Anbieter aller Sprachmodellketten): leitet die Anfrage an einen von OpenRouter eingesetzten Inferenz-Anbieter weiter, beschränkt auf Anbieter ohne Speicherung und ohne Training (Abschnitt D)	EU-Standardvertragsklauseln gemäß Data Processing Agreement des Anbieters (Unternehmensvereinbarung; wird dem Auftraggeber auf Verlangen vorgelegt); OpenRouter speichert Eingaben und Ausgaben nicht; ergänzende Maßnahmen nach Abschnitt D	Datenschutzerklärung Nutzungsbedingungen Datenerhebung und Speicherung Betriebsart ohne Speicherung (Zero Data Retention) Umgang der Inferenz-Anbieter mit Eingaben Trust Center (DPA, Unterauftragsverarbeiter)
6	Mistral AI SAS 15 rue des Halles, 75001 Paris, Frankreich	Frankreich (EU)	Multimodales Modell für hochgeladene Bilder und gescannte Dokumentseiten (erster Anbieter)	Nicht erforderlich (Verarbeitung in der EU); Data Processing Addendum des Anbieters; Trainingsausschluss im Konto des Auftragnehmers eingestellt	Data Processing Addendum Datenschutzerklärung Unterauftragsverarbeiter

Nr.	Anbieter	Sitz	Zweck (Kette und Position)	Drittland-Schutzmaßnahme	Verbindliche Unterlagen
7	Groq UK Limited (Vertragspartner für Kunden im EWR; Betrieb durch Groq LLC, Mountain View, USA) 3 Hammersmith Grove, London W6 0ND, Vereinigtes Königreich	Vereinigtes Königreich / USA	Multimodales Modell für Bilder und Scans (zweiter Anbieter)	Angemessenheitsbeschluss der EU-Kommission für das Vereinigte Königreich; für die Weiterverarbeitung in den USA EU-Standardvertragsklauseln (Modul 2 und 3) gemäß Data Processing Addendum des Anbieters; Betriebsart ohne Speicherung; ergänzende Maßnahmen nach Abschnitt D	Data Processing Addendum Nutzungsvereinbarung Datenumgang der Schnittstelle Unterauftragsverarbeitung
8	Cerebras Systems Inc. 1237 E. Arques Avenue, Sunnyvale, CA 94085, USA	USA	Sprachmodell zur Reparatur fehlerhafter Dateien (sechster Anbieter, Reserve)	EU-Standardvertragsklauseln gemäß Data Processing Agreement des Anbieters (nicht öffentlich; wird dem Auftraggeber auf Verlangen vorgelegt); keine Speicherung von Eingaben und Ausgaben nach der Datenschutzerklärung; ergänzende Maßnahmen nach Abschnitt D	Nutzungsbedingungen Datenschutzerklärung Trust Center (DPA, Unterauftragsverarbeitung)

Abrufdatum der verlinkten Unterlagen: 26.08.2026. Übermittelt werden in jeder Anfrage nur die in Abschnitt B genannten Daten.

D. Ergänzende Maßnahmen

- Übermittlung ausschließlich TLS-verschlüsselt; keine Übermittlung von E-Mail-Adressen, Passwörtern, Zahlungs- und Rechnungsdaten (Abschnitt B).
- Kein Training: Die übermittelten Inhalte werden von keinem Anbieter zum Training von KI-Modellen verwendet (vertragliche Zusicherung des jeweiligen Anbieters bzw. entsprechende Einstellung im Konto des Auftragnehmers; Unterlagen in Abschnitt C).
- Keine Speicherung der Eingaben, soweit angeboten: Fireworks.ai, Baseten, Together, Deep Infra, Cerebras und OpenRouter speichern Eingaben und Ausgaben nach ihren Bedingungen nicht über die Bearbeitung der Anfrage hinaus; bei Groq ist die Betriebsart ohne Speicherung im Konto des Auftragnehmers aktiviert; Mistral AI hält Eingaben und Ausgaben nach seiner

Datenschutzerklärung höchstens 30 Tage zur Missbrauchskontrolle vor; bei OpenRouter ist die Weiterleitung auf Inferenz-Anbieter ohne Speicherung und ohne Training beschränkt.

- Feste Ketten und Beschränkung: Je Zweck werden nur die in Abschnitt A genannten Anbieter angesprochen; im Programmcode der Plattform sind keine weiteren Anbieter eingebunden. Ein weiterer Anbieter wird nicht ohne Information nach § 10 Abs. 5 hinzugezogen.
- Zugangsschlüssel zu den Anbietern liegen ausschließlich serverseitig beim Auftragnehmer; Anfragen tragen keine Kennung des Nutzers oder des Auftraggebers gegenüber dem Anbieter, sondern nur die Inhalte nach Abschnitt B.
- Kontrolle: Der Auftragnehmer prüft die Bedingungen der Anbieter regelmäßig und dokumentiert Änderungen im Änderungsvermerk dieses Vertrages.

Änderungsvermerk

Revision	Stand	Änderungen
Revision 00	August 2026	Erstfassung des Auftragsverarbeitungsvertrags für Norminator (bisher auf Anfrage). Aufbau nach dem Muster des AVV Rechtskataster.com (Revision 01) mit Anlagen 1–4; § 10a und Anlage 4 beschreiben die KI-Verarbeitung durch acht Anbieter in festen Ketten, den Datenumfang je Anfrage, die Web-Recherche sowie Speicherung und Löschung.

Dieser Auftragsverarbeitungsvertrag ist ein Standard-Vertrag der Privates Institut für Qualität und Innovation GmbH (IQI) für die Nutzung der Plattform Norminator. Die rechtliche Prüfung im Einzelfall obliegt dem Auftraggeber. IQI erbringt keine Rechtsdienstleistungen im Sinne des RDG.