Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DSGVO (AVV)

für die Nutzung der Plattform „Compliance Check" (compliance.rit.services)

Version 1.1 · Stand 2026-11-02 · Aufbau entlang der „Checkliste Prüfung AVV" (Version 1.0) der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI). Die Zuordnung Prüfpunkt → Paragraph steht in der Datei `Checkliste-BlnBDI-Pruefung-AVV.md`.

---

zwischen

dem **Kunden** (die Organisation, die im Registrierungsprozess der Plattform „Compliance Check" benannt wird)

— nachfolgend **„Verantwortlicher"** oder **„Auftraggeber"** (AG) —

und

RIT Services GmbH
Am alten Güterbahnhof 57
50825 Köln, Deutschland
Amtsgericht Köln, HRB 115067 · USt-ID DE367518494
vertreten durch den Geschäftsführer Matthias Wessner

— nachfolgend **„Anbieter"** oder **„Auftragsverarbeiter"** (AN) —

— gemeinsam die **„Parteien"** —

Präambel

Der Anbieter stellt dem Kunden die Software-as-a-Service-Plattform **„Compliance Check"** (https://compliance.rit.services) zur Verfügung. Die Plattform übersetzt den EU AI Act, die DSGVO und weitere Gesetze mit KI-Bezug in Deutschland in Checklisten: Sie stuft KI-Systeme des Kunden über einen Fragebogen in Risikoklassen ein, erzeugt daraus Anforderungslisten, verwaltet Aufgaben und Zuständigkeiten im Team des Kunden und dokumentiert den Bearbeitungsstand. Die Nutzung ist unentgeltlich. Grundlage der Nutzung sind die Nutzungsbedingungen, die der Kunde im Registrierungsprozess annimmt (nachfolgend **„Hauptvertrag"**).

Beim Betrieb der Plattform verarbeitet der Anbieter personenbezogene Daten im Auftrag des Kunden. Die Unentgeltlichkeit lässt die datenschutzrechtlichen Pflichten der Parteien unberührt.

Diese Vereinbarung ist ein **Vertrag** im Sinne von Art. 28 Abs. 3 UAbs. 1 S. 1 DSGVO und für beide Parteien rechtlich bindend.

---

§ 1 Gegenstand und Dauer der Verarbeitung

1.1 Gegenstand

Gegenstand der Verarbeitung ist die Bereitstellung und der Betrieb der Plattform „Compliance Check" für den Kunden, umfassend:

a) Bereitstellung der webbasierten Anwendung zur Risikoeinstufung von KI-Systemen, zur Erzeugung und Bearbeitung von Compliance-Checklisten, zum Gesetzes-Explorer sowie zu Erinnerungen an fällige Prüfungen;
b) Verwaltung der Organisation des Kunden und der Benutzerkonten seiner Nutzer:innen (Registrierung, Einladung, Authentifizierung einschließlich optionaler Zwei-Faktor-Authentifizierung, Rollen Inhaber/Admin/Mitglied);
c) Speicherung und Verarbeitung der vom Kunden und seinen Nutzer:innen eingegebenen Inhalte (Beschreibungen von KI-Systemen, Antworten auf Einstufungsfragen, Checklisten, Datenschutzprofile, Aufgaben, Kommentare, hochgeladene Dokumente);
d) Führung des Aktivitätsverlaufs (Protokollierung von Änderungen und Zuständigkeiten);
e) Versand transaktionaler System-E-Mails (Verifizierung, Einladungen, Benachrichtigungen, Erinnerungen);
f) Bereitstellung von Datenexporten und Löschfunktionen;
g) technischer Betrieb, Wartung, Datensicherung (Backups), Störungsbeseitigung und Support.

Die Einzelheiten sind in **Anlage 1** festgelegt.

1.2 Dauer

Die Verarbeitung beginnt mit Abschluss dieser Vereinbarung im Registrierungsprozess und dauert an, **solange der Anbieter personenbezogene Daten für den Kunden tatsächlich verarbeitet**, längstens bis zur vollständigen Löschung oder Rückgabe aller personenbezogenen Daten nach § 12. Die Kündigung oder Beendigung des Hauptvertrags beendet diese Vereinbarung nicht; sie gilt für alle danach fortgesetzten Verarbeitungen (insbesondere Export, Rückgabe, Löschung, Überschreiben von Sicherungskopien) fort.

---

§ 2 Art und Zweck der Verarbeitung

2.1 Art der Verarbeitung

Die Verarbeitung umfasst (Art. 4 Nr. 2 DSGVO) das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung an die berechtigten Nutzer:innen des Kunden, den Abgleich, die Einschränkung, das Löschen und die Vernichtung personenbezogener Daten, jeweils im Rahmen des Betriebs der Plattform. Sie erfolgt ausschließlich automatisiert innerhalb der Plattform; manuelle Zugriffe des Anbieters erfolgen nur zur Störungsbeseitigung oder auf Weisung des Kunden im Support-Fall.

2.2 Zweck der Verarbeitung

Zweck der Verarbeitung ist, dem Kunden zu ermöglichen, KI-Systeme in seiner Organisation nach EU AI Act, DSGVO und weiteren einschlägigen Gesetzen einzustufen, die daraus folgenden Anforderungen als

Checklisten zu bearbeiten, Zuständigkeiten und Fristen zu verwalten und den Erfüllungsstand nachzuweisen; einschließlich Benutzer- und Organisationsverwaltung, Benachrichtigung, Datensicherung und Support.

Eine Verarbeitung zu eigenen Zwecken des Anbieters findet nicht statt. Insbesondere werden Auftragsdaten **nicht** zum Training von KI-Modellen, zu Produkt- oder Nutzungsanalysen auf Personenebene, zu Werbezwecken oder zur Weitergabe an Dritte außerhalb der Anlage 3 verwendet.

Die Einzelheiten sind in **Anlage 1** festgelegt.

---

§ 3 Art der personenbezogenen Daten

Gegenstand der Verarbeitung sind folgende Datenkategorien:

a) **Konto- und Stammdaten der Nutzer:innen:** Name, geschäftliche E-Mail-Adresse, Rolle in der Organisation (Inhaber/Admin/Mitglied), Sprache, Zeitpunkt der Registrierung;
b) **Authentifizierungsdaten:** Passwort (ausschließlich als gesalzener Hash), Faktoren der Zwei-Faktor-Authentifizierung, Session-Token, Verifizierungs- und Einladungstoken;
c) **Organisationsdaten mit Personenbezug:** Namen und Kontaktdaten von Ansprechpartner:innen, Verantwortlichen und Aufgabeninhaber:innen (z. B. Verantwortliche für ein KI-System oder eine Checklistenaufgabe);
d) **Inhaltsdaten:** Beschreibungen von KI-Systemen, Antworten auf Einstufungsfragen, Checklisteneinträge, Datenschutzprofile, Aufgaben, Kommentare und hochgeladene Dokumente, soweit sie Personenbezug aufweisen;
e) **Nutzungs- und Protokolldaten:** Aktivitätsverlauf (wer hat wann was geändert), Anmeldezeitpunkte, IP-Adressen und technische Serverprotokolle;
f) **Benachrichtigungsdaten:** Inhalte und Empfänger:innen von System-E-Mails und In-App-Benachrichtigungen;
g) **Supportdaten:** Inhalte von Supportanfragen einschließlich Kontaktdaten der anfragenden Person.

Die Plattform ist nicht für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) bestimmt. Der Kunde stellt sicher, dass solche Daten nicht in Freitextfelder eingegeben oder als Dokumente hochgeladen werden.

Die Einzelheiten sind in **Anlage 1** festgelegt.

---

§ 4 Kategorien betroffener Personen

a) Beschäftigte und sonstige Nutzer:innen des Kunden mit Benutzerkonto in der Plattform;
b) Beschäftigte des Kunden, die in Inhalten als Ansprechpartner:innen, Verantwortliche oder Aufgabeninhaber:innen genannt werden;
c) externe Personen (z. B. Beschäftigte von Dienstleistern oder Beratern des Kunden), soweit der Kunde sie einlädt oder in Inhalten erfasst;
d) Personen, die in hochgeladenen Dokumenten des Kunden genannt werden.

Die Einzelheiten sind in **Anlage 1** festgelegt.

---

§ 5 Abschluss, Form, Geltung und Rangfolge

5.1 Zwingender Abschluss

Für den Produktivbetrieb wird diese Vereinbarung **zwingend im Registrierungsprozess** oder in den Einstellungen geschlossen; ohne Annahme durch eine vertretungsberechtigte Person des Kunden ist er nicht möglich. Sie gilt für sämtliche Verarbeitungen personenbezogener Daten, die der Anbieter im Auftrag des Kunden durchführt, auch für solche nach Kündigung oder Beendigung des Hauptvertrags (§ 1.2). Ausgenommen sind Testkonten, in denen keine echten personenbezogenen Daten erlaubt sind.

5.2 Form

Die Vereinbarung wird in einem **elektronischen Format** im Sinne von Art. 28 Abs. 9 DSGVO geschlossen. Der Kunde kann die Vereinbarung **einschließlich aller Anlagen jederzeit vollständig als PDF-Datei** aus den Organisationseinstellungen der Plattform herunterladen. Nach Abschluss übermittelt der Anbieter dem Kunden zusätzlich ein vollständiges Exemplar (einschließlich aller Anlagen) an die E-Mail-Adresse der abschließenden Person. Der Anbieter speichert die abgeschlossene Fassung mit Zeitstempel, Angaben zur abschließenden Person und Versionsnummer dauerhaft.

5.3 Bestandteile

Folgende Anlagen sind Bestandteil dieser Vereinbarung und werden ihr formgerecht beigefügt:

- **Anlage 1** — Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen
- **Anlage 2** — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)
- **Anlage 3** — Genehmigte Unterauftragsverarbeiter

Verweise auf den Hauptvertrag, ein Verzeichnis von Verarbeitungstätigkeiten oder sonstige Dokumente ersetzen keine Pflichtangabe dieser Vereinbarung; alle Pflichtangaben nach Art. 28 Abs. 3 DSGVO sind in dieser Vereinbarung und ihren Anlagen selbst enthalten.

5.4 Rangfolge

Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag oder sonstigen Vereinbarungen gehen die Regelungen dieser Vereinbarung vor. Regelungen des Hauptvertrags, die die datenschutzrechtlichen Pflichten des Anbieters oder die Rechte des Kunden aus dieser Vereinbarung einschränken würden, finden insoweit keine Anwendung. Vereinbarte Standardvertragsklauseln der EU-Kommission gehen dieser Vereinbarung vor (§ 16.3).

---

§ 6 Weisungen

6.1 Weisungsbindung

Der Anbieter verarbeitet die personenbezogenen Daten **nur auf dokumentierte Weisung des Kunden, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation**, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Anbieter unterliegt, hierzu verpflichtet ist.

6.2 Mitteilungspflicht bei entgegenstehendem Recht

Ist der Anbieter durch das Recht der Union oder der Mitgliedstaaten zu einer Verarbeitung verpflichtet, die von den Weisungen des Kunden abweicht, teilt er dem Kunden diese rechtlichen Anforderungen **vor der Verarbeitung** mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

6.3 Erteilung und Dokumentation von Weisungen

Diese Vereinbarung einschließlich ihrer Anlagen ist die anfängliche dokumentierte Weisung; sie umfasst auch die Weisung zur Einschaltung der in Anlage 3 genannten Unterauftragsverarbeiter und zu den dort beschriebenen Übermittlungen. Weitere Weisungen erteilt der Kunde

a) durch Nutzung der Selbstbedienungsfunktionen der Plattform (z. B. Einladen und Entfernen von Nutzer:innen, Anlegen, Ändern und Löschen von Inhalten, Datenexport, Löschung von Konto oder Organisation) oder
b) in Textform an die in § 6.4 genannte Adresse.

Mündlich erteilte Weisungen bestätigt der Kunde unverzüglich in Textform. **Der Anbieter dokumentiert alle Weisungen und ihre Umsetzung.** Weisungen über Plattformfunktionen werden im Aktivitätsverlauf systemseitig protokolliert; Weisungen in Textform werden vom Anbieter zusammen mit ihrer Umsetzung abgelegt.

6.4 Weisungsberechtigte und Weisungsempfänger

Weisungsberechtigt sind die Nutzer:innen des Kunden mit der Rolle „Inhaber" oder „Admin". Weisungsempfänger des Anbieters ist der Support der RIT Services GmbH, E-Mail info@rit.services. Änderungen der weisungsberechtigten Personen nimmt der Kunde über die Rollenverwaltung der Plattform vor.

6.5 Kosten

Die Befolgung von Weisungen ist **unentgeltlich**. Nur Weisungen, die über die vertraglichen Vereinbarungen hinausgehen und auch nicht erforderlich sind, um Rechtsverstöße im Zuständigkeitsbereich des Anbieters zu verhindern oder abzustellen, kann der Anbieter nach vorheriger Ankündigung nach Aufwand vergüten lassen. Die Weisungsbindung bleibt hiervon unberührt.

6.6 Keine Verarbeitung zu eigenen Zwecken

Der Anbieter verarbeitet Auftragsdaten nicht zu eigenen Zwecken und behält sich keine Rechte an ihnen vor. Das gilt auch für Protokoll- und Telemetriedaten mit Personenbezug; diese werden ausschließlich für den sicheren Betrieb der Plattform im Auftrag des Kunden verarbeitet.

---

§ 7 Remonstrationspflicht

Ist der Anbieter der Auffassung, dass eine Weisung des Kunden gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, **informiert er den Kunden unverzüglich**. Der Anbieter ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis der Kunde sie bestätigt oder ändert.

---

§ 8 Vertraulichkeit

Der Anbieter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen **zur Vertraulichkeit verpflichtet haben** oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung gilt zeitlich unbeschränkt und über das Ende der jeweiligen Tätigkeit hinaus. Der Anbieter weist die Verpflichtung dem Kunden auf Verlangen nach.

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

9.1 Verpflichtung nach Art. 32 DSGVO

Der Anbieter ergreift **alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen**, um unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

9.2 Konkrete Maßnahmen und dynamische Anpassung

Die bei Vertragsschluss getroffenen Maßnahmen sind in **Anlage 2** beschrieben. Der Anbieter passt diese Maßnahmen **fortlaufend an den Stand der Technik und die Risikolage an**; das in Anlage 2 beschriebene Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert der Anbieter und teilt sie dem Kunden per E-Mail an die Adressen der Nutzer:innen mit der Rolle „Inhaber" mit.

§ 10 Unterstützung bei den Rechten der betroffenen Personen

10.1 Unterstützungspflicht

Der Anbieter unterstützt den Verantwortlichen **angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen**. Dies umfasst alle Rechte aus **Art. 12 bis 22 DSGVO** (Transparenz und Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Mitteilungspflicht, Datenübertragbarkeit, Widerspruch, automatisierte Entscheidungen im Einzelfall).

10.2 Selbstbedienungsfunktionen

Die Plattform stellt hierfür Selbstbedienungsfunktionen bereit: Einsicht und Berichtigung von Konto- und Inhaltsdaten, vollständiger Datenexport der Organisation in einem gängigen maschinenlesbaren Format, Löschung einzelner Inhalte, Löschung von Benutzerkonten und Löschung der gesamten Organisation. Soweit ein Antrag damit nicht erfüllt werden kann, unterstützt der Anbieter auf Weisung des Kunden im Einzelfall.

10.3 Anfragen betroffener Personen beim Anbieter

Wendet sich eine betroffene Person unmittelbar an den Anbieter, leitet dieser das Ersuchen unverzüglich an den Kunden weiter und beantwortet es nicht selbst, es sei denn, der Kunde weist ihn hierzu an.

10.4 Kosten

Die Unterstützung erfolgt **unentgeltlich**.

---

§ 11 Unterstützung bei den Pflichten aus Art. 32 bis 36 DSGVO

11.1 Unterstützungspflicht

Der Anbieter unterstützt den Verantwortlichen **unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten**, also bei der Sicherheit der Verarbeitung (Art. 32), der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33), der Benachrichtigung der betroffenen Personen (Art. 34), der Datenschutz-Folgenabschätzung (Art. 35) und der vorherigen Konsultation der Aufsichtsbehörde (Art. 36).

11.2 Meldung von Datenschutzverletzungen

Der Anbieter meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten, die Auftragsdaten betrifft, **unverzüglich** nach Bekanntwerden per E-Mail an die Nutzer:innen mit der Rolle „Inhaber" und teilt die ihm verfügbaren Informationen im Sinne von Art. 33 Abs. 3 DSGVO mit; Informationen, die zunächst nicht vorliegen, reicht er ohne unangemessene Verzögerung nach.

11.3 Kosten

Die Unterstützung erfolgt **unentgeltlich**.

---

§ 12 Löschung und Rückgabe nach Abschluss der Verarbeitung

12.1 Grundsatz

Der Anbieter **löscht oder gibt nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurück und löscht die vorhandenen Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.**

12.2 Ausübung des Wahlrechts

Der Kunde übt sein Wahlrecht jederzeit über die Plattform aus: Rückgabe durch die Exportfunktion (vollständiger Export der Organisation in einem gängigen maschinenlesbaren Format), Löschung durch die Funktion „Organisation löschen". Er kann beides kombinieren (erst exportieren, dann löschen).

12.3 Vorabregelung bei fehlender Wahl

Ist die Erbringung der Verarbeitungsleistungen abgeschlossen (z. B. Kündigung des Hauptvertrags durch eine Partei), ohne dass der Kunde eine Wahl getroffen hat, fordert der Anbieter die Nutzer:innen mit der Rolle „Inhaber" per E-Mail zur Wahl auf. Erfolgt innerhalb von 30 Tagen keine Wahl, löscht der Anbieter die Daten. Bis zur tatsächlichen Löschung kann der Kunde die Wahl jederzeit ändern und den Export abrufen.

12.4 Umfang und Durchführung der Löschung

a) Die Löschpflicht erfasst **alle personenbezogenen Daten** einschließlich Kopien, Sicherungskopien und Protokolldaten, auch bei Unterauftragsverarbeitern.
b) Bei Löschung der Organisation vernichtet der Anbieter den organisationsspezifischen Verschlüsselungsschlüssel und löscht die Datensätze in der Produktivumgebung unverzüglich.
c) Daten in rollierenden, verschlüsselten Sicherungskopien werden spätestens **30 Tage** nach der Löschung in der Produktivumgebung überschrieben. Bis dahin gelten diese Vereinbarung und die Maßnahmen der Anlage 2 für die Sicherungskopien fort; eine Wiederherstellung aus Sicherungskopien erfolgt nur zur Störungsbeseitigung und führt nicht zur Wiederherstellung gelöschter Organisationen.
d) Die Löschung erfolgt nach dem Stand der Technik; auf Verlangen bestätigt der Anbieter sie dem Kunden in Textform.

12.5 Gesetzliche Speicherpflichten und Nachweisdokumentation

Besteht nach dem Unionsrecht oder dem Recht eines Mitgliedstaats eine Verpflichtung zur Speicherung, beschränkt der Anbieter die Verarbeitung der betroffenen Daten auf Zweck und Dauer dieser Pflicht und löscht sie danach unaufgefordert. Dokumentation zum Nachweis der ordnungsgemäßen Verarbeitung (z. B. Abschlussfassung dieser Vereinbarung, Weisungsprotokoll) bewahrt der Anbieter nur auf, soweit sie keine Auftragsdaten enthält oder eine gesetzliche Aufbewahrungspflicht besteht.

---

§ 13 Nachweispflichten

Der Anbieter **stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung**. Dazu gehören insbesondere die Dokumentation der Maßnahmen nach Anlage 2, das Weisungsprotokoll, Nachweise der Vertraulichkeitsverpflichtungen, die Verträge mit Unterauftragsverarbeitern nach § 15.5 in Bezug auf die Datenschutzpflichten sowie Prüfberichte und Testate, soweit vorhanden. Vertraulichkeitspflichten des Kunden gegenüber dem Anbieter hindern den Kunden nicht daran, diese Nachweise gegenüber Aufsichtsbehörden und betroffenen Personen zu führen. Die Nachweiserbringung ist **unentgeltlich**.

---

§ 14 Kontrollrechte

14.1 Grundsatz

Der Anbieter **ermöglicht Überprüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt dazu bei**. Kontrollen umfassen auch Vor-Ort-Prüfungen in den Betriebsstätten des Anbieters während der üblichen

Geschäftszeiten sowie die Einsicht in die relevanten Systeme und Unterlagen. Sie können sich auch auf Tätigkeiten von Unterauftragsverarbeitern erstrecken (§ 15.5).

14.2 Ablauf

a) Kontrollen erfolgen **in der Regel nach vorheriger Anmeldung** mit angemessener Frist. Einer vorherigen Anmeldung bedarf es nicht, wenn andernfalls der Kontrollzweck gefährdet wäre.
b) Der Kunde kann die Kontrolle selbst oder durch einen von ihm beauftragten Prüfer durchführen. Der Prüfer darf nicht in unmittelbarem Wettbewerbsverhältnis zum Anbieter stehen.
c) Kontrollen dürfen nicht zu übermäßigen Beeinträchtigungen des Geschäftsablaufs des Anbieters führen. Das hindert den Prüfer nicht, sich ein umfassendes Bild vom Gegenstand der Prüfung zu machen und sich von der Einhaltung der Pflichten des Anbieters zu überzeugen; bei konkreten Anhaltspunkten für Verstöße sind auch erhebliche Beeinträchtigungen nicht übermäßig.
d) Der Anbieter kann Kontrollen durch aussagekräftige Unterlagen (Dokumentation nach Anlage 2, Prüfberichte, Testate der Unterauftragsverarbeiter) unterstützen. Solche Unterlagen ergänzen Kontrollen, ersetzen sie aber nicht.

14.3 Kosten

Kontrollmitwirkung ist **unentgeltlich**.

---

§ 15 Unterauftragsverarbeiter

15.1 Allgemeine schriftliche Genehmigung

Der Kunde erteilt dem Anbieter die **allgemeine schriftliche Genehmigung** im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, Unterauftragsverarbeiter nach Maßgabe dieses § 15 in Anspruch zu nehmen. Die Beauftragung von Unterauftragsverarbeitern, die nicht in Anlage 3 genannt oder nach § 15.3 und § 15.4 hinzugekommen sind, ist unzulässig; Bereichsausnahmen (z. B. für Wartung) bestehen nicht.

15.2 Bestimmtheit

Die bei Vertragsschluss genehmigten Unterauftragsverarbeiter sind in **Anlage 3** vollständig aufgeführt, jeweils mit Firma einschließlich Rechtsform, Anschrift, stichwortartiger Beschreibung des Aufgabenbereichs, Abgrenzung der Aufgaben gegenüber den anderen Unterauftragsverarbeitern, Ort der Verarbeitung und Übermittlungsgrundlage. Ein Verweis auf eine Liste auf einer Website ersetzt Anlage 3 nicht.

15.3 Information über beabsichtigte Änderungen

Der Anbieter informiert den Kunden über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters **vorab und aktiv per E-Mail** an die Nutzer:innen mit der Rolle „Inhaber", unter Angabe von Firma einschließlich Rechtsform, Anschrift, stichwortartiger Beschreibung des Aufgabenbereichs, Abgrenzung zu den bestehenden Unterauftragsverarbeitern, Ort der Verarbeitung und Übermittlungsgrundlage. Eine In-App-Benachrichtigung oder die Veröffentlichung auf einer Website genügt nicht.

15.4 Einspruch

Der Kunde kann der Änderung innerhalb von **28 Tagen** nach Zugang der Information widersprechen. Vor Ablauf dieser Frist und bei fristgerechtem Einspruch wird der neue Unterauftragsverarbeiter für Daten des Kunden nicht eingesetzt. Bei Einspruch suchen die Parteien eine einvernehmliche Lösung (z. B. Verzicht auf den Unterauftragsverarbeiter für diesen Kunden). Kommt sie nicht zustande, kann jede Partei den Hauptvertrag und diese Vereinbarung mit einer Frist von 30 Tagen beenden; bis zur Beendigung stehen dem Kunden der vollständige Datenexport und die Rechte aus § 12 zu. Eine Entgeltpflicht besteht nicht.

15.5 Pflichten der Unterauftragsverarbeiter

Der Anbieter erlegt jedem Unterauftragsverarbeiter im Wege eines Vertrags **dieselben Datenschutzpflichten auf, die in dieser Vereinbarung festgelegt sind**, insbesondere hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Der Anbieter stellt sicher, dass jeder Unterauftragsverarbeiter alle Pflichten erfüllt, denen der Anbieter nach dieser Vereinbarung und der DSGVO unterliegt. Die Nachweis- und Kontrollrechte des Kunden nach § 13 und § 14 gelten auch für die Tätigkeiten der Unterauftragsverarbeiter; der Anbieter stellt die hierfür erforderlichen vertraglichen Rechte sicher und übt sie auf Verlangen des Kunden aus. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Anbieter gegenüber dem Kunden für die Einhaltung der Pflichten des Unterauftragsverarbeiters (Art. 28 Abs. 4 S. 2 DSGVO).

15.6 Nebenleistungen

Leistungen Dritter ohne Zugriff auf Auftragsdaten (z. B. Telekommunikationsdienste als reine Transportleistung, Reinigung, Wartung von Hardware ohne Datenzugriff) sind keine Unterauftragsverarbeitung. Auch insoweit trifft der Anbieter angemessene Vertraulichkeits- und Schutzvorkehrungen.

---

§ 16 Verarbeitungsort und Übermittlung in Drittländer

16.1 Verarbeitung in der EU

Die Verarbeitung der Auftragsdaten in der Plattform (Anwendung, Datenbank, Dateispeicher, Sicherungskopien) erfolgt ausschließlich auf einem vom Anbieter selbst betriebenen Kubernetes-Cluster, dessen Server in Rechenzentren in Mitgliedstaaten der Europäischen Union stehen (Deutschland und Finnland, siehe Anlage 3).

16.2 Übermittlung an Drittländer

Eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, einschließlich Fernzugriffen aus Drittländern, erfolgt nur

a) auf dokumentierte Weisung des Kunden (§ 6.1, § 6.3) **und**
b) wenn die Voraussetzungen des Kapitels V der DSGVO erfüllt sind, also ein Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO die Übermittlung deckt, oder Standardvertragsklauseln der Europäischen Kommission nach dem Durchführungsbeschluss (EU)

2021/914 in dem für die Konstellation passenden Modul vereinbart sind, oder verbindliche interne Datenschutzvorschriften nach Art. 47 DSGVO vorliegen, **und**
c) wenn der Anbieter bei Übermittlungen auf Grundlage von Standardvertragsklauseln oder verbindlichen internen Datenschutzvorschriften durch eine dokumentierte Prüfung der Rechtslage im Drittland (Transfer Impact Assessment) und erforderlichenfalls ergänzende Maßnahmen sichergestellt hat, dass ein dem Unionsrecht gleichwertiges Schutzniveau gewährleistet ist, insbesondere im Hinblick auf Zugriffe von Behörden.

Die bei Vertragsschluss bestehenden Übermittlungen sind in Anlage 3 beschrieben:

a) Versand transaktionaler E-Mails durch einen in den USA ansässigen Unterauftragsverarbeiter, der nach dem EU-U.S. Data Privacy Framework zertifiziert ist und ergänzend Standardvertragsklauseln vereinbart hat (Anlage 3 Nr. 4);

b) Fernzugriff eines mit dem Anbieter verbundenen Unternehmens in Pakistan (Anlage 3 Nr. 5) zur Administration der Infrastruktur und zur Bearbeitung von Support-Fällen. Die Infrastrukturadministration erfolgt ohne Zugriff auf die Schlüssel der Feld- und Datenträgerverschlüsselung, sodass für die Administrator:innen nur verschlüsselte Daten erreichbar sind. Support-Mitarbeiter:innen dieses Unternehmens erhalten Daten ausschließlich in pseudonymisierter Form über ein vom Anbieter in der EU betriebenes Gateway, nur für die betreffende Organisation, nur nach deren Freigabe für einen konkreten Support-Fall und nur für dessen Dauer; die Zuordnung zu Klardaten verbleibt beim Anbieter in der EU. Grundlage sind Standardvertragsklauseln 2021/914 Modul 3 mit dokumentiertem Transfer Impact Assessment; Verschlüsselung ohne Schlüsselzugriff und Pseudonymisierung sind die ergänzenden Maßnahmen im Sinne der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses (Anwendungsfälle 1 und 2). Einen Klartextzugriff durch Personen außerhalb der EU gibt es nicht;

c) Verarbeitung pseudonymisierter Datenauszüge aus freigegebenen Support-Fällen durch einen KI-Dienst in den USA (Anlage 3 Nr. 6), den die Support-Mitarbeiter:innen des Anbieters als Arbeitswerkzeug einsetzen; Grundlage sind Standardvertragsklauseln 2021/914 Modul 3 mit dokumentiertem Transfer Impact Assessment und der Pseudonymisierung als ergänzender Maßnahme.

Der Kunde kann die Übermittlungen nach lit. b) und c) für Support-Fälle in den Einstellungen seiner Organisation ausschließen („Support-Zugriff von außerhalb der EU zulassen", Voreinstellung: nein); die Infrastrukturadministration nach lit. b) auf verschlüsselten Daten bleibt davon unberührt. Der Anbieter überwacht den Fortbestand der Zertifizierungen und des Angemessenheitsbeschlusses und informiert den Kunden nach § 15.3, wenn sich eine Übermittlungsgrundlage ändert.

16.3 Keine Einschränkung von Standardvertragsklauseln

Vereinbarte Standardvertragsklauseln werden durch diese Vereinbarung weder eingeschränkt noch geändert; im Konfliktfall gehen sie vor. Insbesondere werden Kontrollrechte, Löschpflichten und die Haftung des Datenimporteurs aus den Standardvertragsklauseln nicht beschränkt.

---

§ 17 Rechenschaftspflicht und Auslegung

Die Parteien beachten die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Diese Vereinbarung ist so auszulegen und anzuwenden, dass die Anforderungen des Art. 28 DSGVO stets vollständig erfüllt sind. Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen

Bestimmungen unberührt; an die Stelle der unwirksamen Bestimmung tritt die wirksame Regelung, die den Anforderungen des Art. 28 DSGVO am nächsten kommt.

§ 18 Schlussbestimmungen

a) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines elektronischen Formats im Sinne von Art. 28 Abs. 9 DSGVO; das gilt auch für diese Klausel. Über Änderungen informiert der Anbieter die Nutzer:innen mit der Rolle „Inhaber" vorab per E-Mail; die geänderte Fassung wird erst mit Annahme durch eine vertretungsberechtigte Person des Kunden wirksam und ist danach vollständig als PDF herunterladbar. Frühere Fassungen bleiben abrufbar.
b) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit zulässig, Köln.
c) Einreden und Zurückbehaltungsrechte des Anbieters in Bezug auf die Auftragsdaten, insbesondere hinsichtlich Herausgabe, Export und Löschung, sind ausgeschlossen.
d) Ein Datenschutzbeauftragter ist beim Anbieter nicht benannt, da keine Benennungspflicht besteht. Ansprechpartner für Datenschutzfragen ist die Geschäftsführung der RIT Services GmbH, E-Mail info@rit.services.

Abschluss der Vereinbarung

Die Vereinbarung wird im Registrierungsprozess elektronisch geschlossen (Art. 28 Abs. 9 DSGVO). Die Plattform erfasst und speichert:

Angabe	Wert
Kunde (Verantwortlicher)	Firma, Rechtsform, Anschrift (Eingabe im Registrierungsprozess)
Abschließende, vertretungsberechtigte Person	Name, Funktion, E-Mail-Adresse
Bestätigung der Vertretungsberechtigung	Pflicht-Checkbox
Zeitpunkt des Abschlusses	Zeitstempel (UTC)
Fassung	Version 1.1 vom 2026-11-02
Anbieter (Auftragsverarbeiter)	RIT Services GmbH, Am alten Güterbahnhof 57, 50825 Köln, vertreten durch den Geschäftsführer Matthias Wessner

Anlage 1 — Gegenstand, Dauer, Art und Zweck der Verarbeitung, Datenarten und Kategorien betroffener Personen

Gegenstand: Bereitstellung und Betrieb der Plattform „Compliance Check" (https://compliance.rit.services) für die Organisation des Kunden: Risikoeinstufung von KI-Systemen per Fragebogen, Erzeugung und Bearbeitung von Compliance-Checklisten, Gesetzes-Explorer, Aufgaben-

und Zuständigkeitsverwaltung, Erinnerungen, Aktivitätsverlauf, Dokumenten-Upload, Organisations- und Benutzerverwaltung, System-E-Mails, Datenexport und Löschung, Backup, Support.

Dauer: Ab Abschluss der Vereinbarung im Registrierungsprozess, solange der Anbieter personenbezogene Daten für den Kunden tatsächlich verarbeitet, längstens bis zur vollständigen Löschung oder Rückgabe aller Daten einschließlich Sicherungskopien (§ 1.2, § 12).

Art der Verarbeitung (Art. 4 Nr. 2 DSGVO): Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung/Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung an berechtigte Nutzer:innen des Kunden, Abgleich, Einschränkung, Löschen, Vernichtung; automatisiert innerhalb der Plattform.

Zweck: Einstufung, Dokumentation und Nachweis der Compliance von KI-Systemen des Kunden nach EU AI Act, DSGVO und weiteren Gesetzen; Team- und Aufgabenverwaltung; Benachrichtigung; technischer Betrieb einschließlich Backup und Störungsbeseitigung; Support. Keine Verarbeitung zu eigenen Zwecken des Anbieters, kein KI-Training mit Auftragsdaten.

Art der personenbezogenen Daten:

Nr.	Datenkategorie	Konkretisierung	Aufbewahrung in der Plattform
1	Konto-/Stammdaten	Name, geschäftliche E-Mail-Adresse, Rolle (Inhaber/Admin/Mitglied), Sprache, Registrierungszeitpunkt	bis Löschung des Kontos oder der Organisation
2	Authentifizierungsdaten	Passwort-Hash, Zwei-Faktor-Faktoren, Session-Token, Verifizierungstoken, Einladungstoken	Verifizierungstoken 7 Tage, Einladungen 90 Tage, sonst bis Löschung des Kontos
3	Organisationsdaten mit Personenbezug	Ansprechpartner:innen, Verantwortliche für KI-Systeme und Aufgaben	bis Löschung durch den Kunden oder der Organisation
4	Inhaltsdaten	Beschreibungen von KI-Systemen, Einstufungsantworten, Checklisten, Datenschutzprofile, Aufgaben, Kommentare, hochgeladene Dokumente (feldweise verschlüsselt, Anlage 2)	bis Löschung durch den Kunden oder der Organisation
5	Nutzungs-/Protokolldaten	Aktivitätsverlauf, Anmeldezeitpunkte, IP-Adressen, Serverprotokolle	Aktivitätsverlauf 365 Tage rollierend, spätestens mit Löschung der Organisation
6	Benachrichtigungsdaten	Inhalt und Empfänger:innen von System-E-Mails und In-App-Benachrichtigungen	In-App-Benachrichtigungen 180 Tage
7	Supportdaten	Inhalt und Kontaktdaten aus Supportanfragen	bis Abschluss der Anfrage, längstens bis Löschung der Organisation

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand des Auftrags; der Kunde stellt sicher, dass solche Daten nicht eingegeben oder hochgeladen werden.

Kategorien betroffener Personen:

Nr.	Kategorie
1	Beschäftigte und sonstige Nutzer:innen des Kunden mit Benutzerkonto
2	Beschäftigte des Kunden, die in Inhalten als Ansprechpartner:innen, Verantwortliche oder Aufgabeninhaber:innen genannt werden
3	Externe Personen (Dienstleister, Berater), die der Kunde einlädt oder in Inhalten erfasst
4	Personen, die in hochgeladenen Dokumenten des Kunden genannt werden

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand 2026-09-07. Der Anbieter ist derzeit nicht nach ISO 27001 oder SOC 2 zertifiziert; die Maßnahmen werden durch Dokumentation und Kontrollen nach § 13 und § 14 nachgewiesen.

1. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a)

- Transportverschlüsselung des gesamten Datenverkehrs zwischen Browser und Anwendung sowie zwischen Anwendung und Unterauftragsverarbeitern mit TLS; Zertifikate werden automatisiert erneuert.
- Verschlüsselung der Datenträger und Datenbank-Volumes im Ruhezustand (Encryption at Rest); die Schlüssel liegen ausschließlich beim Anbieter, nicht bei den Rechenzentrumsbetreibern.
- Zusätzliche **Feldverschlüsselung sensibler Inhalte mit AES-256-GCM und einem eigenen Schlüssel je Organisation** (Beschreibungen von KI-Systemen, Checklisten, Datenschutzprofile, hochgeladene Dokumente). Bei Löschung der Organisation wird der Schlüssel vernichtet (Crypto-Shredding).
- Passwörter werden ausschließlich als gesalzener Hash nach dem Stand der Technik gespeichert; Token sind zufällig erzeugt und zeitlich befristet (Anlage 1).
- Sicherungskopien werden verschlüsselt gespeichert.
- **Schlüsseltrennung:** Die Schlüssel der Feld- und Datenträgerverschlüsselung sowie die Zugangsdaten der Datenbanken werden in einer vom Produktiv-Cluster getrennten Umgebung verwaltet, auf die ausschließlich Mitarbeiter:innen des Anbieters in der EU Zugriff haben. Anwendungen beziehen Schlüssel zur Laufzeit über einen authentifizierten Kanal; Schlüssel werden nicht in Konfigurationsdateien, Container-Images oder Cluster-Secrets abgelegt.
- **Pseudonymisierung im Support:** Support-Zugriffe von Mitarbeiter:innen außerhalb der EU (Anlage 3 Nr. 5) erfolgen ausschließlich über ein in der EU betriebenes Gateway, das alle personenbezogenen Felder vor der Ausgabe durch fallbezogene, nicht umkehrbare Ersatzwerte ersetzt (HMAC mit je Support-Fall abgeleitetem Schlüssel), Freitexte, Dokumente und besondere Kategorien nach Art. 9 DSGVO nicht ausgibt und die Abfrage auf die freigebende Organisation begrenzt.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b)

- *Zutrittskontrolle:* Betrieb ausschließlich auf dedizierten Servern in Rechenzentren der in Anlage 3 genannten Betreiber in der EU mit physischen Zutrittskontrollen (Zutrittskontrollsystem, Videoüberwachung, Besucherprotokollierung, 24/7-Bewachung); der Anbieter selbst betreibt keine

eigenen Serverräume. Die Betreiber haben keinen logischen Zugriff; physischer Zugriff auf Datenträger führt wegen der Verschlüsselung nicht zu lesbaren Daten.

- *Plattformbetrieb:* eigener Kubernetes-Cluster des Anbieters auf diesen Servern; Cluster-Zugänge nur über verschlüsselte, authentifizierte Verbindungen; Konfiguration versioniert und nachvollziehbar.
- *Zugangskontrolle:* personenbezogene Benutzerkonten; optionale Zwei-Faktor-Authentifizierung für Nutzer:innen des Kunden; Zwei-Faktor-Authentifizierung und Schlüssel-basierter Zugang für Administrationszugänge des Anbieters; Passwortrichtlinie; Sitzungsablauf; kein geteiltes Administrationskonto.
- *Zugriffskontrolle:* rollenbasiertes Berechtigungsmodell in der Plattform (Inhaber, Admin, Mitglied) nach dem Need-to-know-Prinzip; Administrationszugriffe des Anbieters auf die Geschäftsführung und benannte Administrator:innen beschränkt und protokolliert. Infrastrukturadministration durch Anlage 3 Nr. 5 ohne Schlüssel- und Datenbankzugang; Änderungen am Produktivsystem nur über versionierte, signierte Auslieferungen mit Freigabe durch eine Person des Anbieters in der EU; kein interaktiver Zugriff auf laufende Anwendungscontainer.
- *Support-Zugriff:* Zugriff auf Auftragsdaten einer Organisation im Support nur nach Freigabe durch Inhaber oder Admin dieser Organisation für einen benannten Fall, zeitlich befristet (Voreinstellung 72 Stunden, höchstens 14 Tage) und jederzeit widerrufbar; Freigaben, Widerrufe und alle Abfragen werden protokolliert, die Organisation erhält nach Ablauf einen Zugriffsbericht; Klartextzugriff nur durch Mitarbeiter:innen des Anbieters in der EU; Zugriff von außerhalb der EU nur pseudonymisiert (Nr. 1) und nur, wenn die Organisation ihn in ihren Einstellungen zugelassen hat.
- *Trennungskontrolle:* logische Mandantentrennung je Organisation in Datenbank und Dateispeicher, zusätzlich kryptografisch durch den Schlüssel je Organisation; getrennte Entwicklungs-, Test- und Produktivumgebungen; keine Produktivdaten in Entwicklungs- oder Testsystemen.

3. Integrität (Art. 32 Abs. 1 lit. b)

- *Weitergabekontrolle:* verschlüsselte Übertragung; Datenexporte nur durch berechtigte Nutzer:innen des Kunden und protokolliert; keine Weitergabe an Dritte außerhalb der Anlage 3.
- *Eingabekontrolle:* Aktivitätsverlauf mit Protokollierung von Anlage, Änderung und Löschung von Inhalten sowie Änderungen von Zuständigkeiten und Rollen (Aufbewahrung 365 Tage).

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c)

- tägliche automatisierte, verschlüsselte Sicherungskopien mit Aufbewahrung von 30 Tagen an einem vom Produktivsystem getrennten Speicherort innerhalb der EU;
- regelmäßig getestete Wiederherstellung einschließlich der verschlüsselten Felder;
- Monitoring und Alarmierung des Produktivbetriebs; Schutz vor Überlastung und unautorisierten Zugriffen (Rate Limiting, Firewall);
- dokumentiertes Wiederanlaufverfahren.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d)

- Patch- und Schwachstellenmanagement für Anwendung, Abhängigkeiten und Betriebssystem; sicherheitsrelevante Updates werden zeitnah eingespielt;
- Überprüfung dieser Maßnahmen mindestens jährlich sowie anlassbezogen;
- Incident-Response-Verfahren mit Meldeweg nach § 11.2 (Art. 33 und 34 DSGVO);

- Auftragskontrolle: Auswahl der Unterauftragsverarbeiter nach hinreichenden Garantien, Abschluss von Verträgen nach § 15.5, regelmäßige Überprüfung ihrer Nachweise (Zertifikate, Prüfberichte, Zertifizierung nach dem Data Privacy Framework).

6. Datenschutzorganisation

- Ansprechpartner für Datenschutz: Geschäftsführung der RIT Services GmbH (Matthias Wessner), E-Mail info@rit.services; kein Datenschutzbeauftragter benannt, da keine Benennungspflicht besteht;
- Verpflichtung aller Beschäftigten auf Vertraulichkeit (§ 8), regelmäßige Sensibilisierung;
- interne Regelungen zu Berechtigungsvergabe, Löschung, Umgang mit Sicherheitsvorfällen und Einsatz von Unterauftragsverarbeitern;
- Betroffenenrechte im Selbstbedienungsprinzip in der Plattform umgesetzt (§ 10.2).

Anlage 3 — Genehmigte Unterauftragsverarbeiter

Betriebsmodell: Der Anbieter betreibt die Plattform auf einem eigenen Kubernetes-Cluster. Die Cluster-Knoten sind dedizierte Server, die der Anbieter bei den unter Nr. 1 bis 3 genannten Rechenzentrumsbetreibern mietet. Diese Betreiber stellen ausschließlich Hardware, Rechenzentrum, Stromversorgung und Netzanbindung bereit; sie haben keinen logischen Zugriff auf Betriebssystem, Cluster, Datenbanken oder Anwendungsdaten. Datenträger und Datenbanken sind verschlüsselt (Anlage 2 Nr. 1), sodass auch ein physischer Zugriff auf die Hardware keinen Zugriff auf lesbare Daten ermöglicht. Der Anbieter führt die Betreiber vorsorglich als Unterauftragsverarbeiter, weil sie physischen Zugang zu den Datenträgern haben.

Die Administration des Clusters und die erste Bearbeitung von Support-Fällen erfolgen teilweise durch das mit dem Anbieter verbundene Unternehmen unter Nr. 5 im Wege des Fernzugriffs aus Pakistan. Die Schlüssel der Feld- und Datenträgerverschlüsselung sowie die Zugangsdaten der Datenbanken liegen in einer getrennten, ausschließlich von Mitarbeiter:innen des Anbieters in der EU verwalteten Umgebung; Administrator:innen unter Nr. 5 können deshalb nur verschlüsselte Daten erreichen. Support-Anfragen aus Pakistan laufen ausschließlich über ein in dieser EU-Umgebung betriebenes Gateway, das die Freigabe der Organisation prüft, die Abfrage auf diese Organisation begrenzt, alle personenbezogenen Felder vor der Ausgabe pseudonymisiert (fallbezogene, nicht umkehrbare Ersatzwerte; Freitexte, Dokumente und besondere Kategorien werden nicht ausgegeben), Abfragemengen begrenzt und jede Abfrage protokolliert. Klartextzugriff im Support ist Mitarbeiter:innen des Anbieters in der EU vorbehalten und setzt ebenfalls die Freigabe der Organisation voraus.

Nr.	Firma (einschließlich Rechtsform)	Anschrift	Aufgabenbereich (stichwortartig) und Abgrenzung	Ort der Verarbeitung	Übermittlungsgrundlage
1	Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Vermietung dedizierter Server als Knoten des Kubernetes-Clusters des Anbieters (Hardware, Rechenzentrum, Netzanbindung); kein logischer Zugriff auf Daten	Rechenzentren Nürnberg und Falkenstein (Deutschland), Helsinki (Finnland)	entfällt (EU)

Nr.	Firma (einschließlich Rechtsform)	Anschrift	Aufgabenbereich (stichwortartig) und Abgrenzung	Ort der Verarbeitung	Übermittlungsgrundlage
2	IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Deutschland	Vermietung dedizierter Server als Knoten des Kubernetes-Clusters des Anbieters (Hardware, Rechenzentrum, Netzanbindung); kein logischer Zugriff auf Daten	Rechenzentren in Deutschland	entfällt (EU)
3	STRATO GmbH	Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland	Vermietung dedizierter Server als Knoten des Kubernetes-Clusters des Anbieters (Hardware, Rechenzentrum, Netzanbindung); kein logischer Zugriff auf Daten. Zusätzlich DNS-Verwaltung der Domain rit.services (keine Auftragsdaten)	Rechenzentren Berlin und Karlsruhe (Deutschland)	entfällt (EU)
4	Plus Five Five, Inc. (Marke „Resend")	2261 Market Street #5039, San Francisco, CA 94114, USA	Versand transaktionaler System-E-Mails (Verifizierung, Einladungen, Benachrichtigungen, Erinnerungen); verarbeitet ausschließlich E-Mail-Adresse, Anzeigename und Inhalt der jeweiligen System-E-Mail; keine Inhaltsdaten der Plattform	USA	Angemessenheitsbeschluss EU-U.S. Data Privacy Framework (Empfänger zertifiziert); ergänzend Standardvertragsklauseln 2021/914 Modul 3 (Auftragsverarbeiter an Unterauftragsverarbeiter) im Data Processing Addendum des Empfängers; Transfer Impact Assessment beim Anbieter dokumentiert

Nr.	Firma (einschließlich Rechtsform)	Anschrift	Aufgabenbereich (stichwortartig) und Abgrenzung	Ort der Verarbeitung	Übermittlungsgrundlage
5	Rasalhague IT Services (Private) Limited	Office No. B4, Plot No. 398, Service Road E, I-9/3, Islamabad 44000, Islamabad Capital Territory, Pakistan (SECP Corporate Unique Identification No. 0266092)	Verbundenes Unternehmen des Anbieters. (a) Administration des Kubernetes-Clusters und der Systemsoftware im Fernzugriff **ohne Zugriff auf Verschlüsselungsschlüssel und Datenbank-Zugangsdaten**, daher nur auf verschlüsselte Daten; (b) Bearbeitung von Support-Fällen ausschließlich mit **pseudonymisierten Datenauszügen** über das Gateway des Anbieters, nur nach Freigabe der betreffenden Organisation für einen konkreten Fall und für dessen Dauer. Kein Klartextzugriff, keine Speicherung von Auftragsdaten in Pakistan	Fernzugriff aus Pakistan auf Systeme in der EU (Nr. 1 bis 3); die Daten verbleiben in der EU	Standardvertragsklauseln 2021/914 Modul 3 (Auftragsverarbeiter an Unterauftragsverarbeiter) zwischen Anbieter und Nr. 5; Transfer Impact Assessment beim Anbieter dokumentiert; ergänzende Maßnahmen: Verschlüsselung ohne Schlüsselzugriff (Administration) und Pseudonymisierung mit Zuordnung nur in der EU (Support), jeweils nach EDSA-Empfehlungen 01/2020

Nr.	Firma (einschließlich Rechtsform)	Anschrift	Aufgabenbereich (stichwortartig) und Abgrenzung	Ort der Verarbeitung	Übermittlungsgrundlage
6	Anthropic Ireland, Limited (Vertragspartner für Kunden im EWR); Verarbeitung durch deren Muttergesellschaft und Sub-Prozessor Anthropic, PBC, 548 Market Street, PMB 90375, San Francisco, CA 94104, USA	6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland (CRO 760497)	KI-Assistenzdienst („Claude"), den Support-Mitarbeiter:innen des Anbieters und von Nr. 5 als Arbeitswerkzeug bei der Fallbearbeitung nutzen; verarbeitet ausschließlich die **pseudonymisierten Datenauszüge** aus dem Gateway (Nr. 5 lit. b) und die Eingaben der Support-Mitarbeiter:innen; keine Klardaten, keine Dokumente der Plattform; Nutzung über die kommerzielle Programmierschnittstelle ohne Verwendung der Daten zum Modelltraining, mit Zero-Data-Retention-Vereinbarung und einem Modell ohne Sicherheitsaufbewahrung	USA (Infrastruktur von Anthropic, PBC)	Weiterübermittlung von Anthropic Ireland, Limited an Anthropic, PBC: Standardvertragsklauseln 2021/914 Modul 3 (Auftragsverarbeiter an Unterauftragsverarbeiter) im Data Processing Addendum von Anthropic mit Pseudonymisierung als ergänzender Maßnahme; Transfer Impact Assessment beim Anbieter dokumentiert. Anthropic, PBC ist nicht nach dem EU-U.S. Data Privacy Framework zertifiziert (Stand 2026-09-07)

Abgrenzung: Nr. 1 bis 3 erbringen dieselbe Leistungsart (Bereitstellung dedizierter Hardware) für jeweils unterschiedliche, dem Anbieter namentlich zugeordnete Server desselben Clusters; welche Workloads (Anwendung, Datenbank, Dateispeicher, Sicherungskopien) auf welchem Knoten laufen, steuert allein der Anbieter. Nr. 4 ist der einzige Unterauftragsverarbeiter mit Zugriff auf Klardaten (E-Mail-Adresse, Name, Text der jeweiligen System-E-Mail). Nr. 5 verwaltet die Systeme ohne Schlüsselzugriff und erhält im Support nur pseudonymisierte Auszüge; Nr. 6 erhält ausschließlich diese pseudonymisierten Auszüge als Werkzeug der Support-Bearbeitung und hat keinen Zugang zu den Systemen des Anbieters. Nr. 4 bis 6 sind die Unterauftragsverarbeiter, bei denen eine Verarbeitung oder ein Zugriff außerhalb der EU stattfindet (§ 16.2). Nicht aufgeführte Dienstleister werden für Auftragsdaten des Kunden nicht eingesetzt.