

Ontaric GmbH

Resourcecloud

Datenschutz- und Sicherheitspaket

Unterlagen für Vergabe- und Beschaffungsverfahren öffentlicher Auftraggeber

Version 1.0 · Stand 05.10.2026

Ontaric GmbH · Jürgen-Töpfer-Straße 113 · 22763 Hamburg

datenschutz@resourcecloud.io

Inhalt

1. Kurzfassung
2. Muster-Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO
3. Anlage 1 – Technisch-organisatorische Maßnahmen (TOM)
4. Anlage 2 – Unterauftragsverarbeiter und Hosting-Standorte
5. Anlage 3 – Beschreibung des lokalen KI-Betriebs
6. Anlage 4 – Löschkonzept

Kurzfassung

Hosting in Deutschland

Anwendungsinstanzen bei Contabo (Nürnberg), Backups bei Hetzner (Nürnberg) und STRATO (Deutschland). Keine Verarbeitung in Drittländern im Standardbetrieb.

Eine Instanz je Kunde

Eigene Datenbank, eigenes Dateivolumen, eigenes Netz. Kein gemeinsamer Datenbestand mit anderen Kunden.

KI lokal oder gar nicht

Embeddings und Reranking laufen auf dem Server der Instanz. Im Modus „nur lokal“ lehnt die Anwendung jeden Endpunkt außerhalb des lokalen Netzes ab.

Starke Anmeldung

Passkeys und Zwei-Faktor, SAML-2.0-Single-Sign-On, SCIM-Provisionierung, Sperrverzögerung bei Fehlversuchen.

Klares Löschkonzept

Definierte Fristen je Datenkategorie, Rückgabe der Daten und nachweisbare Löschung zum Vertragsende.

Muster-AV-Vertrag

Art. 28 DSGVO, mit Anlagen. Auf Wunsch passen wir ihn an Ihr Vertragsmuster an.

Die folgenden Abschnitte sind zugleich die Anlagen des Muster-AV-Vertrags. Sie beschreiben den Stand des Produkts und des Betriebs zum angegebenen Datum. Wo eine Maßnahme vom Kunden zu konfigurieren oder zu aktivieren ist, steht das ausdrücklich dabei.

Muster-Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO)

zwischen dem im Hauptvertrag genannten Auftraggeber (**Verantwortlicher**, nachfolgend „Auftraggeber“)
und der Ontaric GmbH, Jürgen-Töpfer-Straße 113, 22763 Hamburg (**Auftragsverarbeiter**, nachfolgend „Auftragnehmer“).

Dieser Vertrag ist ein Muster. Er gilt, wenn der Auftragnehmer Resourcecloud für den Auftraggeber betreibt (gehostete Instanz) oder im Rahmen von Support Zugriff auf personenbezogene Daten des Auftraggebers erhält. Beim reinen Selbstbetrieb durch den Auftraggeber ohne Zugriff des Auftragnehmers ist er nicht erforderlich.

§ 1 Gegenstand, Dauer und Art der Verarbeitung

1. Der Auftragnehmer stellt dem Auftraggeber die Anwendung Resourcecloud (Aufgaben-, Projekt-, Ressourcen- und Zeitverwaltung einschließlich optionaler KI-Funktionen) als gehostete, ausschließlich dem Auftraggeber zugeordnete Instanz bereit und betreibt sie. Näheres regelt der Hauptvertrag.
2. Die Verarbeitung umfasst Speichern, Bereitstellen, Sichern, Aktualisieren und Löschen der Daten sowie Support und Fehleranalyse auf Weisung des Auftraggebers.
3. Die Dauer entspricht der Laufzeit des Hauptvertrags. § 9 und Anlage 4 regeln das Vertragsende.
4. Arten personenbezogener Daten: Stammdaten der Nutzer (Name, Benutzername, E-Mail, Rolle, Team), Anmelde- und Nutzungsdaten (Anmeldezeiten, Fehlversuche, Sitzungsdaten), Arbeitsdaten mit Personenbezug (Zuweisungen, Zeiterfassung, Abwesenheiten, Kommentare, Dateianhänge), Kontaktdaten externer Ansprechpartner und Kunden des Auftraggebers sowie Inhalte, die der Auftraggeber selbst in die Anwendung einträgt. Besondere Kategorien nach Art. 9 DSGVO sind nicht vorgesehen. Der Auftraggeber stellt sicher, dass er solche Daten nicht ohne gesonderte Abstimmung einträgt.
5. Kreis der Betroffenen: Beschäftigte und sonstige Nutzer des Auftraggebers, externe Ansprechpartner und Kunden des Auftraggebers sowie Dritte, deren Daten der Auftraggeber in der Anwendung erfasst.

§ 2 Weisungsrecht

1. Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, er ist durch Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Auftraggeber die rechtliche Anforderung vorab mit, sofern das Recht dies nicht verbietet.
2. Der Hauptvertrag, dieser Vertrag und die Konfiguration der Anwendung durch den Auftraggeber sind die Weisungen. Einzelweisungen erfolgen in Textform. Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn er eine Weisung für rechtswidrig hält. Er darf ihre Ausführung bis zur Bestätigung oder Änderung aussetzen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet die Daten nicht für eigene Zwecke. Die Daten werden nicht zum Training von KI-Modellen verwendet.

2. Er verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit oder stellt sicher, dass sie einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).
3. Er trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen und entwickelt sie weiter. Wesentliche Verschlechterungen des Schutzniveaus sind unzulässig. Änderungen, die das Niveau erhöhen oder erhalten, bedürfen keiner Zustimmung. Die jeweils aktuelle Fassung wird auf Anfrage und auf der Trust-Seite bereitgestellt.
4. Er führt ein Verzeichnis der Verarbeitungstätigkeiten für Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO).
5. Datenschutzkontakt des Auftragnehmers: datenschutz@resourcecloud.io.
6. Die Verarbeitung findet ausschließlich in Deutschland statt (Anlage 2). Eine Verlagerung in einen anderen Staat setzt eine vorherige Zustimmung des Auftraggebers in Textform voraus und die Voraussetzungen der Art. 44 ff. DSGVO müssen erfüllt sein.

§ 4 Unterstützung des Auftraggebers

1. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Mitteln bei der Beantwortung von Anträgen betroffener Personen (Art. 12–22 DSGVO). Anträge, die direkt beim Auftragnehmer eingehen, leitet er unverzüglich weiter und beantwortet sie nicht selbst. Auskunft, Berichtigung, Einschränkung und Löschung kann der Auftraggeber in der Anwendung selbst durchführen. Der Datenexport ist über die Anwendung und die REST-Schnittstelle möglich.
2. Er unterstützt bei der Einhaltung der Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation der Aufsichtsbehörde), soweit es um Informationen und Verarbeitungsvorgänge in seinem Verantwortungsbereich geht.
3. Vertraulichkeit und Aufwand: Unterstützung im Rahmen der gewöhnlichen Betriebsabläufe ist im Entgelt enthalten. Darüber hinausgehender Aufwand wird nur nach vorheriger Abstimmung berechnet.

§ 5 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die seinen Verantwortungsbereich oder den eines Unterauftragsverarbeiters betrifft, unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntnis. Die Meldung enthält, soweit bekannt, Art der Verletzung, betroffene Daten und Personen, wahrscheinliche Folgen und ergriffene oder vorgeschlagene Maßnahmen. Fehlende Angaben werden nachgereicht. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung der Betroffenen sind Sache des Auftraggebers.

§ 6 Unterauftragsverarbeitung

1. Der Auftraggeber erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter.
2. Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor dem Einsatz eines neuen oder dem Austausch eines Unterauftragsverarbeiters in Textform. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen widersprechen. Bleibt der Widerspruch ungelöst, kann jede Partei den betroffenen Teil des Hauptvertrags zum Zeitpunkt des Einsatzes außerordentlich kündigen.
3. Der Auftragnehmer schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem Vertrag entsprechende Datenschutzpflichten auferlegt. Er haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragsverarbeiter seine Pflichten erfüllt.

4. Dienstleistungen ohne Zugriff auf personenbezogene Daten des Auftraggebers (Anlage 2, Abschnitt C) sind keine Unterauftragsverhältnisse.

§ 7 Kontrollrechte

1. Der Auftragnehmer weist die Einhaltung seiner Pflichten durch die Unterlagen dieses Pakets und auf Anfrage durch weitere Auskünfte nach. Der Auftraggeber kann sich außerdem vor Ort oder per Fernzugriff überzeugen. Prüfungen werden mit angemessener Frist (in der Regel 14 Tage) angekündigt, während der üblichen Geschäftszeiten und ohne Störung des Betriebs durchgeführt. Der Prüfer unterliegt der Vertraulichkeit.
2. Soweit Rechenzentren der Unterauftragsverarbeiter betroffen sind, gelten deren Zutrittsregeln. Der Auftragnehmer stellt die ihm vorliegenden Nachweise der Unterauftragsverarbeiter zur Verfügung.
3. Aufsichtsbehörden können nach geltendem Recht prüfen. Der Auftragnehmer unterstützt dabei.

§ 8 Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Betroffenenrechte verantwortlich. Er konfiguriert die Anwendung seinen Anforderungen entsprechend, insbesondere die Rollen und Berechtigungen, die Anmeldeverfahren und die optionalen Dienste (KI, Avatare, Chat-Erweiterungen). Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 9 Rückgabe und Löschung

1. Nach Vertragsende gibt der Auftragnehmer dem Auftraggeber nach dessen Wahl alle Daten in einem gängigen, maschinenlesbaren Format heraus und löscht sie anschließend, einschließlich vorhandener Kopien, nach Maßgabe von Anlage 4. Die Löschung wird auf Anforderung schriftlich bestätigt.
2. Gesetzliche Aufbewahrungspflichten bleiben unberührt. Davon betroffene Daten werden gesperrt und nur zu diesem Zweck verwendet.

§ 10 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Innenverhältnis gelten die Haftungsregelungen des Hauptvertrags, soweit zwingendes Recht nicht entgegensteht.

§ 11 Schlussbestimmungen

1. Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in Fragen des Datenschutzes vor.
2. Soweit der Auftraggeber an ergänzende Vorgaben des Landesrechts gebunden ist (zum Beispiel Landesdatenschutzgesetz), gelten diese zusätzlich. Die Parteien stimmen erforderliche Anpassungen ab.
3. Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. Es gilt deutsches Recht.

Anlagen

Anlage 1 – Technisch-organisatorische Maßnahmen · Anlage 2 – Unterauftragsverarbeiter und Hosting-Standorte · Anlage 3 – Beschreibung des lokalen KI-Betriebs · Anlage 4 – Löschkonzept

Auftraggeber	Auftragnehmer: Ontaric GmbH
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift

Anlage 1 – Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

Gegliedert nach den Schutzzielen des Art. 32 DSGVO. „Anwendung“ bezeichnet Resourcecloud, „Betrieb“ die Infrastruktur, die der Auftragnehmer für gehostete Instanzen unterhält.

1. Zutrittskontrolle

Maßnahme	Umsetzung
Rechenzentren	Server und Backup-Speicher stehen in Rechenzentren der Unterauftragsverarbeiter (Anlage 2). Zutrittskontrolle, Videoüberwachung, Brandschutz und Stromversorgung liegen dort. Der Auftragnehmer betreibt keine eigenen Serverräume für Kundendaten. Die Nachweise der Anbieter stellen wir auf Anfrage zur Verfügung.

2. Zugangskontrolle

Maßnahme	Umsetzung
Authentifizierung der Nutzer	Lokale Konten, LDAP oder Single-Sign-On über SAML 2.0. Zwei-Faktor-Anmeldung und Passkeys (WebAuthn) stehen zur Verfügung. Benutzer lassen sich per SCIM 2.0 aus dem Identitätssystem des Auftraggebers anlegen, ändern und deaktivieren.
Passwörter	Passwörter werden ausschließlich als Hash mit dem Standardverfahren von PHP (derzeit bcrypt) gespeichert, nie im Klartext.
Schutz vor Angriffen auf Anmeldung	Fehlversuche werden je Konto gezählt, die Antwort wird zunehmend verzögert (Zeitfenster und Obergrenze konfigurierbar). Fehlversuchsdaten werden nach 24 Stunden gelöscht.
Sitzungen	Automatische Abmeldung nach Inaktivität (je Instanz einstellbar). Sitzungsdaten liegen in einem eigenen Volume und werden nicht gesichert.
API-Zugriff	Persönliche API-Token werden serverseitig erzeugt und nur als SHA-256-Hash gespeichert. Ein Nutzer kann keine Token für andere Konten erzeugen.
Administrativer Zugriff im Betrieb	Zugriff auf die Server nur für berechtigte Personen des Auftragnehmers über SSH. Der Auslieferungsweg (CI) nutzt ein eigenes Deploy-Konto mit Schlüsselauthentifizierung. Zugangsdaten der Instanzen liegen in nicht öffentlichen Umgebungsdateien je Kunde.

3. Zugriffskontrolle

Maßnahme	Umsetzung
Rollen- und Berechtigungskonzept	Rollenbasierte Rechte, abgestuft nach Team, Organisationseinheit und Leitungsbeziehung. Jeder Endpunkt der Anwendung wird zentral gegen eine Berechtigungsrichtlinie geprüft.
Private Aufgaben	Als privat markierte Aufgaben sehen nur Ersteller und Bearbeiter. Alle Abfragen verwenden dafür gemeinsame Filter.
Sichtbarkeit von Arbeitszeiten	Auslastungs- und Zeitdaten sind nach einem festgelegten Modell nur für berechtigte Führungskräfte sichtbar.
Automatische Prüfung	Eine Regressionstest-Suite und eine Gesundheitsprüfung testen unter anderem rollenübergreifende Zugriffe, Zugriffe zwischen Teams und private Aufgaben. Sie läuft vor Veröffentlichungen in der Auslieferungskette.
Datenbankzugriff	Datenbankabfragen der Anwendung sind parametrisiert. Die Datenbank ist von außen nicht erreichbar.

4. Trennungskontrolle

Maßnahme	Umsetzung
Mandantentrennung	Jeder Kunde erhält ein eigenes Compose-Projekt mit eigener Datenbank, eigenem Dateivolumen, eigenem Scheduler und privatem Netz. Nur der Web-Container ist an das gemeinsame Edge-Netz angebunden, daher ist die Datenbank eines Kunden aus den Containern eines anderen nicht erreichbar.
Lizenzserver	Getrennter Dienst ohne Zugriff auf Instanzdatenbanken, ohne Docker-Zugriff und ohne Host-Zugriff. Er erhält nur die in Anlage 2 genannten Meldungen.

5. Weitergabekontrolle

Maßnahme	Umsetzung
Transportverschlüsselung	Alle Zugriffe auf die Anwendung laufen über HTTPS. Der Reverse-Proxy (Traefik) beendet TLS mit automatisch erneuerten Zertifikaten und leitet jeden HTTP-Aufruf auf HTTPS um. Die Übertragung zu den Backup-Speichern (S3) erfolgt über TLS-Endpunkte.
Browser-Schutzmaßnahmen	Strenge Content-Security-Policy mit Nonce (kein unsafe-inline, kein eval), X-Frame-Options, X-Content-Type-Options: nosniff und Referrer-Policy. Formulare und Ajax-Aufrufe sind durch CSRF-Token geschützt.
E-Mail	Versand über den SMTP-Server der Instanz. Standardmäßig ist das der Mailserver des Auftragnehmers (Standort Hamburg), der Auftraggeber kann einen eigenen SMTP-Server eintragen (mit TLS). E-Mails liegen nur bis zum Versand in der Warteschlange.
Datenträger und Datenaustausch	Datenexport über die Anwendung oder REST-Schnittstelle. Eine Weitergabe an Dritte erfolgt nur auf Weisung des Auftraggebers.

6. Eingabekontrolle

Maßnahme	Umsetzung
Nachvollziehbarkeit	Anmeldezeiten, Änderungsprotokolle für Projekte sowie die Autorennzuordnung von Kommentaren und Aufgaben sind in der Anwendung gespeichert.
Betriebsprotokolle	Der Auslieferungsweg protokolliert, welches Image (Commit) pro Instanz in Betrieb ist.

7. Auftragskontrolle

Maßnahme	Umsetzung
Weisungsbindung	Verarbeitung nur nach dem AV-Vertrag und dokumentierten Weisungen. Mitarbeitende sind zur Vertraulichkeit verpflichtet.
Unterauftragnehmer	Auswahl nach Standort und Sicherheitsniveau, vertragliche Bindung nach Art. 28 DSGVO, Liste in Anlage 2.

8. Verfügbarkeit und Belastbarkeit

Maßnahme	Umsetzung
Datensicherung	Je Instanz werden Datenbank, Uploads und Avatare sowie die Zertifikate gesichert, die Kundenkonfiguration ebenfalls. Die Sicherungen liegen auf zwei unabhängigen Speichern bei unterschiedlichen Anbietern (Hetzner Object Storage, Nürnberg, und STRATO S3). Aufbewahrung siehe Anlage 4.
Aktualisierung ohne Ausfall	Neue Versionen starten als zusätzliches Replikat. Das alte wird erst entfernt, wenn das neue die Datenbankmigration abgeschlossen hat und gesund ist. Schlägt der Start fehl, bleibt die alte Version in Betrieb. Eine Referenzinstanz („Canary“) wird zuerst aktualisiert.
Datenbankmigrationen	Schemaänderungen laufen ausschließlich über nummerierte Migrationsskripte vor der Auslieferung der Anwendung. Die Anwendung startet nicht ohne passendes Schema.
Überwachung	Healthchecks der Container, Start der abhängigen Dienste erst bei gesunder Datenbank.

9. Datenschutzfreundliche Voreinstellungen und Entwicklung

Maßnahme	Umsetzung
Voreinstellungen	Externe Dienste sind ab Werk aus: Gravatar-Avatare sind standardmäßig deaktiviert, Giphy benötigt einen eigenen Schlüssel, externe KI-Endpunkte sind nicht vorkonfiguriert.
Sichere Entwicklung	Quellcode-Verwaltung und Auslieferung in einer selbst betriebenen GitLab-Instanz. Vor jeder Veröffentlichung laufen automatische Prüfungen in der Auslieferungskette: Syntaxprüfung, statische Analyse (PHPStan), Prüfung auf unmaskierte Ausgaben, Prüfung auf direkte Objektzugriffe (IDOR), Regressions- und Berechtigungstests sowie eine Schema-Prüfung. Ein Image wird erst ausgeliefert, wenn diese Prüfungen bestanden sind und der Start-Test des Images ein funktionierendes Migrations-Gate bestätigt. Abhängigkeiten werden über Paketverwaltung festgelegt.
Geheimnisse	Zugangsdaten werden nicht im Code abgelegt, sondern über Umgebungsvariablen oder die Instanz-Einstellungen bereitgestellt. Die Konfigurationsverzeichnisse der Anwendung sind vom Webzugriff ausgeschlossen. Verzeichnislisting ist abgeschaltet.
Behandlung von Vorfällen	Sicherheitsvorfälle werden dokumentiert und bewertet. Meldung an den Auftraggeber nach § 5 des AV-Vertrags.

Verantwortung des Auftraggebers. Die Wirksamkeit mancher Maßnahmen hängt von der Konfiguration ab: Rollenvergabe, Aktivierung von Zwei-Faktor, Passkeys oder SSO, Sitzungs-Timeout und die Wahl der KI-Endpunkte. Wir beraten bei der Einrichtung und stellen den Anmeldeleitfaden (SSO und SCIM) bereit.

Anlage 2 – Unterauftragsverarbeiter und Hosting-Standorte

A. Unterauftragsverarbeiter (Zugriff auf Auftraggeberdaten)

Unternehmen	Leistung	Daten	Standort
Contabo GmbH, München	Server (VPS) für gehostete Instanzen: Anwendung, Datenbank, Uploads. Hosting des Lizenzservers.	Alle Daten der Instanz	Rechenzentrum Nürnberg, Deutschland
Hetzner Online GmbH, Gunzenhausen	Object Storage (S3) als Backup-Ziel	Sicherungen der Instanz (Datenbank, Uploads)	Nürnberg, Deutschland
STRATO GmbH, Berlin	Object Storage (S3) als zweites Backup-Ziel	Sicherungen der Instanz (Datenbank, Uploads)	Deutschland

Alle Unterauftragsverarbeiter verarbeiten die Daten in Deutschland. Eine Übermittlung in Drittländer findet im Standardbetrieb nicht statt.

B. Eigene Dienste des Auftragnehmers

Dienst	Zweck	Daten
Mailserver (SMTP) des Auftragnehmers, Standort Hamburg	Systemmails der Instanz, sofern der Auftraggeber keinen eigenen SMTP-Server konfiguriert	Empfängeradresse und Inhalt der Benachrichtigung bis zum Versand
Lizenzserver (auf Contabo, siehe A)	Abrechnung der Lizenzen	Pro Monat Anzahl der Sitzplätze und deren Veränderungen, Instanzkennung, Adresse der Instanz. Keine Nutzernamen, keine Arbeitsdaten.

C. Dienste ohne Zugriff auf Auftraggeberdaten

Diese Dienste sind für Betrieb und Bereitstellung nötig, erhalten aber keine personenbezogenen Daten des Auftraggebers. Wir führen sie aus Transparenzgründen auf.

Dienst	Zweck	Was dorthin gelangt
Let's Encrypt (ISRG, USA)	TLS-Zertifikate	Der Hostname der Instanz. Er wird durch Certificate-Transparency-Protokolle öffentlich.
Docker Hub (Docker Inc., USA)	Verteilung der Anwendungs-Images	Nichts aus der Instanz. Der Server lädt Images von dort herunter.
Selbst betriebene GitLab-Instanz des Auftragnehmers	Quellcode, Build und Auslieferung	Nur Code, keine Kundendaten
Hugging Face, Ollama-Modellregister	Einmaliger Download der lokalen KI-Modelle beim ersten Start einer Instanz	Nichts aus der Instanz. Es wird nur heruntergeladen. Danach geht kein KI-Verkehr nach außen (Anlage 3).

D. Optionale Funktionen, die der Auftraggeber aktivieren kann

Standardmäßig deaktiviert. Sie werden nur auf Entscheidung des Auftraggebers wirksam. Der Auftraggeber ist dann Verantwortlicher gegenüber dem jeweiligen Anbieter, der Auftragnehmer ist daran nicht als Unterauftragsverarbeiter beteiligt.

Funktion	Anbieter / Land	Was übertragen wird
Gravatar-Avatare (Einstellung „Gravatar“)	Automattic Inc., USA	Der Browser des Nutzers ruft das Bild ab: Hash der E-Mail-Adresse und IP-Adresse. Behörden sollten die Funktion ausgeschaltet lassen (Voreinstellung).
Giphy-GIFs im Chat (Einstellung „Giphy“, eigener API-Schlüssel nötig)	Giphy, USA	Suchbegriff und Abruf der Bilder
Externer KI-Chat-Endpunkt (z. B. OpenAI, Anthropic Claude)	je nach Anbieter	siehe Anlage 3. Empfohlen wird für Behörden der lokale Betrieb.
Eigener SMTP-Server des Auftraggebers	Auftraggeber	E-Mail-Benachrichtigungen
Externer Dateispeicher (S3) des Auftraggebers	Auftraggeber	Dateianhänge
Kalender-Abo-Link (jede Nutzerin und jeder Nutzer für sich, im Profil)	keiner – der Link wird vom Kalenderprogramm der Person abgerufen	Meetings, Abwesenheiten und eigene Kalendereinträge der Person. Abwesenheiten, auch Krankheit, nur als „Abwesend“, ohne Grund, Art und Kommentar. Der Link ist geheim, nur sein Hash wird gespeichert, und er lässt sich jederzeit widerrufen.
Microsoft-365-Kalender-Synchronisation (Einstellung „Meetings in Outlook-Kalender schreiben“; eigene App-Registrierung des Auftraggebers)	Microsoft, im Mandanten des Auftraggebers	Meetings (Titel, Zeit, Beschreibung, Teilnehmer-Adressen) in die Kalender der Teilnehmer; auf Wunsch Abwesenheiten als ganztägig „Abwesend“, ohne Grund, Art und Kommentar. Die Rechte der App lassen sich per Exchange-Richtlinie auf eine Benutzergruppe beschränken.

Belegtzeiten aus Outlook in die Kapazität (zusätzliche Einstellung; nur mit Zustimmung der einzelnen Person, Voreinstellung aus)	Microsoft, im Mandanten des Auftraggebers	Gelesen wird nur die Frei/Belegt-Information; gespeichert wird ausschließlich die Summe der belegten Minuten je Person und Arbeitstag – nie Titel, Ort, Teilnehmer oder Inhalt. Zeiten, die Resourcecloud selbst kennt, werden nicht noch einmal gezählt. Die Zahlen sind für niemanden einsehbar; die Kapazitätsplanung nennt den Anteil nur für Gruppen ab drei Personen. Für den Betriebsrat: Zustimmung je Person, jederzeit widerrufbar, Löschung sofort.
--	--	--

Anlage 3 – Beschreibung des lokalen KI-Betriebs

Resourcecloud bietet KI-Funktionen (Fragen an den eigenen Datenbestand, Suche, Zusammenfassungen). Für Auftraggeber mit hohem Schutzbedarf läuft die gesamte KI auf eigener Hardware, ohne dass Daten das lokale Netz verlassen.

1. Bausteine

Baustein	Aufgabe	Betrieb
Embedding-Server (Ollama)	Wandelt Texte (Aufgaben, Kommentare, Dateien) in Vektoren um, damit die semantische Suche funktioniert. Modelle: <code>embeddinggemma</code> (Standard) oder <code>bge-m3</code> .	Container in der Instanz, jeder Kunde bringt seinen eigenen mit
Reranker	Sortiert Suchtreffer neu nach Relevanz.	Container in der Instanz
Vektorindex	Speichert die Vektoren zur Suche. Er ist abgeleitet und aus den Originaldaten neu aufbaubar.	In der Datenbank der Instanz (MariaDB, VECTOR-Spalten)
Chat-Modell	Beantwortet Fragen anhand des gefundenen Kontexts.	Vom Auftraggeber festgelegter Endpunkt, siehe Abschnitt 3

2. Betriebsmodus „nur lokal“ (AI_LOCAL_ONLY)

- Der Modus lässt sich bei der Einrichtung der Instanz setzen und in den Einstellungen prüfen.
- Die Anwendung prüft jeden konfigurierten KI-Endpunkt (Chat, Embeddings, Reranker). Löst der Name auf auch nur eine nicht-lokale Adresse auf, wird der Endpunkt abgelehnt. Auch ein Name mit einer öffentlichen und einer privaten Adresse wird abgelehnt.
- Die Verbindung wird an die geprüfte Adresse gebunden. Damit lässt sich die Prüfung nicht dadurch umgehen, dass das DNS kurz danach eine andere Antwort liefert.
- Verweist ein aktiviertes Feature trotzdem nach außen, wird es nicht eingeschaltet. Beim nächsten Start wird erneut geprüft.
- Nach dem ersten Start, bei dem die Modelle einmalig geladen werden, gibt es für Embeddings und Reranking keinen Verkehr nach außen.

3. Chat-Modell: drei Betriebsarten

Betriebsart	Beschreibung	Datenabfluss
Lokal (empfohlen)	Ein Sprachmodell läuft auf Hardware des Auftraggebers oder in dessen Rechenzentrum und wird über eine OpenAI-kompatible Schnittstelle angebunden (zum Beispiel Ollama oder vLLM). Im Modus „nur lokal“ erzwingt die Anwendung das.	Keiner
Extern, vom Auftraggeber freigegeben	Der Auftraggeber trägt einen Endpunkt und Schlüssel eines kommerziellen Anbieters ein (zum Beispiel OpenAI oder Anthropic Claude). Er schließt einen eigenen Vertrag mit dem Anbieter und prüft dessen Standort, Löschfristen und Trainingsnutzung.	Frage und Kontextauszüge gehen an den Anbieter
Aus	Chat deaktiviert. Suche mit lokalen Embeddings bleibt möglich.	Keiner

Voreinstellung. Das Chat-Modell ist nicht vorkonfiguriert. Ohne Entscheidung des Auftraggebers verlässt kein KI-Verkehr die Instanz. Der Auftragnehmer verwendet Kundendaten nicht zum Training. Er stellt weder für gehostete noch für selbst betriebene Instanzen ein Chat-Modell bereit. Bei gehosteten Instanzen betreibt er nur die lokalen Modelle für Embeddings und Reranking. Alles Weitere wählt und richtet der Auftraggeber selbst ein.

4. Welche Daten die KI sieht

- Die Frage des Nutzers und Auszüge aus Datenbeständen der Instanz, die für die Antwort herangezogen werden (zum Beispiel Aufgaben, Projekt- und Teamstatistiken, indizierte Dateien).
- Die KI-Funktionen sind durch Administratoren ein- und ausschaltbar, einzeln für Chat und Suche.
- Embeddings entstehen im Hintergrund durch Wartungsjobs und werden nur lokal erzeugt, sofern die Embedding-Adresse lokal ist (Voreinstellung).

5. Hardwareanforderungen (Richtwerte)

Embedding-Modell etwa 1,1 GB Arbeitsspeicher während der Verarbeitung (bge-m3 etwa 1,7 GB), Reranker etwa 370 MB dauerhaft. Ein lokales Chat-Modell richtet sich nach Modellgröße und Nutzerzahl. Wir beraten bei der Dimensionierung.

Anlage 4 – Löschkonzept

Das Konzept beschreibt, wann welche Daten gelöscht werden, wer löscht und wie. Der Auftraggeber bestimmt als Verantwortlicher, welche Daten er in der Anwendung hält und wie lange. Die Anwendung stellt dafür Löschfunktionen bereit. Der Auftragnehmer löscht darüber hinaus Daten, die er technisch bedingt vorhält.

1. Löschung durch den Auftraggeber in der Anwendung

Datenkategorie	Löschweg	Wirkung
Benutzerkonten	Administrator löscht den Benutzer (nur möglich, wenn mindestens ein weiterer Administrator bleibt).	Konto, Rollen, Teamzuordnung und Ansichtseinstellungen werden sofort entfernt. Offene Aufgaben des Nutzers werden „nicht zugewiesen“.
Arbeitsdaten (Aufgaben, Projekte, Epics, Programme, Kommentare, Kunden, Termine, Releases, Blog-Einträge)	Löschfunktionen je Objekt in der Anwendung, auch als Sammel Löschung für Kommentare und Vorfälle	Sofortige Löschung in der Datenbank
Dateianhänge	Löschen des Anhangs bzw. des Objekts. Beim Zurücksetzen der Instanz wird bei konfiguriertem S3-Speicher der gesamte Bucket-Inhalt der Instanz entfernt.	Datei entfernt
KI-Vektorindex	Abgeleitete Daten. Sie werden bei Änderung der Quelle neu berechnet und lassen sich jederzeit komplett neu aufbauen.	Mit dem Instanzabbau vernichtet

Bearbeitende Personen in abgeschlossenen Datensätzen. Beim Löschen eines Benutzerkontos bleibt die Benutzerkennung als Textverweis in abgeschlossenen Aufgaben und Kommentaren erhalten, damit der Arbeitsverlauf nachvollziehbar bleibt. Fordert der Auftraggeber die Entfernung des Personenbezugs, ersetzt der Auftragnehmer die Kennung in diesen Datensätzen auf Weisung durch eine neutrale Kennung. Die Frist beträgt 30 Tage ab Weisung.

2. Automatische Löschung technisch bedingter Daten

Datenkategorie	Frist	Verfahren
E-Mail-Warteschlange	Sofort nach Versand	Eintrag wird beim erfolgreichen Versand gelöscht
Fehlversuche bei der Anmeldung	24 Stunden (Voreinstellung); bei erfolgreicher Anmeldung sofort für das Konto	Automatisches Aufräumen in der Anwendung
Sitzungsdaten	Ablauf mit dem Sitzungs-Timeout	Eigenes Volume, nicht Teil der Sicherung
Belegzeiten aus Outlook (nur bei aktivierter Funktion und Zustimmung)	Bei Widerruf der Person sofort; beim Abschalten der Funktion beim nächsten Lauf des Planers (Minuten); Werte vergangener Tage täglich; Werte ohne Aktualisierung werden nach drei Tagen nicht mehr verwendet	Automatisches Aufräumen durch den Scheduler; es werden nur Minutensummen je Tag gespeichert
Zuordnung von Terminen zu Outlook-Terminen (Kalender-Synchronisation)	Solange der Termin besteht; Fehlerstände werden mit dem Termin überschrieben	Die Zuordnung enthält keine Terminhalte, nur Kennungen und den Stand der Übertragung

3. Backups

Ziel	Aufbewahrung	Löschung
Hetzner Object Storage (Nürnberg) und STRATO S3	30 Tage rollierend	Ältere Sicherungen werden automatisch durch neuere ersetzt und gelöscht. Gelöschte Daten verschwinden damit spätestens 30 Tage nach der Löschung aus den Sicherungen.

4. Vertragsende und Rückgabe

Schritt	Handlung	Frist
1	Der Auftraggeber fordert die Datenrückgabe an oder nutzt den Export der Anwendung und die REST-Schnittstelle. Auf Wunsch stellt der Auftragnehmer einen Datenbank-Dump und die Dateien bereit.	bis Vertragsende, auf Wunsch bis 30 Tage danach
2	Der Auftragnehmer baut die Instanz ab: Container, Datenbank-Volume, Upload-Volume, Sitzungs-Volume und Umgebungsdatei werden entfernt. Bei S3-Speicher des Auftragnehmers werden die Objekte der Instanz gelöscht.	30 Tage nach Vertragsende bzw. nach bestätigter Rückgabe
3	Sicherungen enthalten die Daten noch bis zum Ablauf der Aufbewahrung (Abschnitt 3).	weitere 30 Tage
4	Auf Anforderung erhält der Auftraggeber eine schriftliche Löschbestätigung. Sie nennt Instanz, Datum und umfasste Datenspeicher.	nach Abschluss

Die Datenträger der Server und Speicher werden von den Rechenzentrumsbetreibern nach deren Verfahren für die Außerbetriebnahme gelöscht. Spätestens 60 Tage nach Vertragsende sind alle Kundendaten bei Auftragnehmer und Unterauftragsverarbeitern entfernt.

5. Daten, die der Auftragnehmer als Verantwortlicher hält

Datenkategorie	Aufbewahrung
Rechnungen, Abrechnungsdaten und Kundenstammdaten der Vertragsparteien im Lizenzserver	Gesetzliche Aufbewahrungsfristen (§ 147 AO, § 257 HGB). Danach Löschung. In der Zwischenzeit sind die Daten gesperrt und werden nur dafür genutzt.
Gemeldete Sitzplatzzahlen und deren Verlauf	Als Beleg der Rechnung wie Rechnungsdaten

Diese Verarbeitung ist keine Auftragsverarbeitung. Sie enthält keine Arbeitsdaten der Instanz.

6. Anfragen betroffener Personen

Anfragen auf Auskunft, Berichtigung oder Löschung leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter. Der Auftragnehmer beantwortet sie nicht selbst. Der Auftraggeber setzt sie in der Anwendung um oder weist den Auftragnehmer an.

Kontakt

Ontaric GmbH

Jürgen-Töpfer-Straße 113

22763 Hamburg

Datenschutz- und Sicherheitsanfragen: datenschutz@resourcecloud.io

Wir senden Ihnen auf Anfrage den Anmeldeleitfaden (SAML und SCIM), weitere Nachweise der Rechenzentrumsbetreiber und den AV-Vertrag in einer an Ihr Muster angepassten Fassung.

Version 1.0 · Stand 05.10.2026. Wir aktualisieren dieses Dokument bei Änderungen an Betrieb, Unterauftragsverarbeitern oder Maßnahmen. Informationen zu Änderungen der Unterauftragsverarbeiter erhalten Auftraggeber nach § 6 des AV-Vertrags in Textform.