CLEVER
CONTRACT INTELLIGENCE

Stand 17. Oktober 2026 · fünfte Fassung

Datensicherheit und Compliance

Dieses Dokument beschreibt, wo Vertragsdaten liegen, wer sie sieht, wohin sie zur Analyse übermittelt werden und was CLEVER ausdrücklich nicht leistet. Jede Angabe nennt den Standard, also die gemeinsame Plattform mit getrennten Mandanten, und die Option, mit der ein Kunde auf Wunsch darüber hinausgeht. Optionen gelten nach Vereinbarung und werden nicht als vorhanden ausgegeben, wo sie es nicht sind.

Gegenstand	Standard (gemeinsame Plattform)	Auf Wunsch (nach Vereinbarung)
Anwendung	über Netlify ausgeliefert, ohne Vertragsdaten	unverändert
Datenbank	ein Supabase-Projekt, Region Frankfurt (AWS eu-central-1), seit 19. September 2026; vorher Irland	eigenes Projekt je Kunde, EU-Region nach Wahl des Kunden
Trennung zwischen Kunden	je Mandant durch eine Datenbankregel auf 39 Tabellen (Entscheid vom 21. September 2026); Probe an einer Kopie des Schemas: keine fremde Zeile sichtbar, in fünf Rollen und zwei Mandanten	eigene Datenbank: kein Abfrageweg zwischen Kunden
Zugriff innerhalb des Mandanten	nach Rolle geregelt (Datenbankregeln je Rolle); ein Deal Manager sieht nur die ihm zugeordneten Verträge	unverändert
Analyse durch Sprachmodell	Anthropic (Vertragspartner: Anthropic Ireland, Limited), Verarbeitung außerhalb des EWR; Löschung der Ein- und Ausgaben innerhalb von 30 Tagen	Verarbeitung in der EU (Amazon Bedrock, Frankfurt) als buchbare Option; wird für den buchenden Kunden eingeschaltet
Training des Modells	ausgeschlossen	ausgeschlossen
Zugriff des Betreibers	technisch möglich über die Datenbank, anlassbezogen; Mitglieder eines Mandanten bestimmt dessen Administrator, nicht der Betreiber	nur nach Freischaltung durch den Kunden
Bewertungslogik	Teil der ausgelieferten Anwendung, ohne Kundendaten	serverseitig bei eigener Instanz

Quellcode	privates Repository	unverändert; bei eigener Instanz erhält der Kunde eine versionierte Fassung
Verschlüsselung	im Transport und im Speicher	unverändert
Zertifizierung	keine	keine
Auftragsverarbeitung	Vereinbarung auf Anfrage	Bestandteil des Vertrags

— Wo CLEVER läuft

Die Anwendung wird über Netlify ausgeliefert und enthält keine Vertragsdaten. Sie lädt diese erst nach der Anmeldung aus der Datenbank. Datenbank und Anmeldung liegen bei Supabase in der Region Frankfurt (AWS eu-central-1), innerhalb der Europäischen Union.

Bis zum 19. September 2026 lag die Datenbank in der Region Irland. Der Bestand ist vollständig nach Frankfurt umgezogen. Das frühere Projekt in Irland ist pausiert, wird nicht mehr genutzt und hält den Stand vom Umzugstag als Rückfallebene.

Die Übermittlung an das Sprachmodell läuft über eine Serverfunktion bei Netlify. Sie reicht den Text durch und protokolliert Tokenzahlen und Laufzeiten, keine Vertragsinhalte.

Welche Dateien die Website ausliefert, regelt eine Freigabeliste. Jeder Ordner ist gesperrt oder ausdrücklich freigegeben; die Prüfung läuft bei jeder Änderung maschinell mit. Am 17. September 2026 wurden dabei vier interne Ordner ohne Kundendaten gefunden, die abrufbar waren. Sie sind gesperrt.

— Mandanten und eigene Instanz

Kunden arbeiten als getrennte Mandanten in einer gemeinsamen Datenbank. Jede der 39 Tabellen mit Kundendaten trägt eine Mandantenkennung, und eine zusätzliche Regel lässt ein Konto nur die Zeilen seines aktiven Mandanten sehen. Die bestehende Rollenlogik gilt darüber unverändert. Die Datenbank setzt die Mandantenkennung selbst und lehnt eine fremde Angabe des Browsers ab. Ein Konto kann Mitglied mehrerer Mandanten sein; welche Mitglieder ein Mandant hat, bestimmt dessen Administrator. Der Betreiber legt Mandanten an (mit einem ersten Administrator) und kann sie stilllegen; er fügt keine Mitglieder hinzu und vergibt keine Rollen. In der Anwendung sieht er keine Mandanteninhalte; der technische Zugriff über die Datenbank ist davon getrennt und im Abschnitt zum Zugriff des Betreibers beschrieben.

Prüfung — am 22. September 2026 wurde die Trennung an einer Kopie des Datenbankschemas mit allen 103 Regeln geprüft: In 39 Tabellen, fünf Rollen und zwei Mandanten war keine fremde Zeile sichtbar (25 von 25 Prüfungen), und die bestehende Rollenlogik blieb unverändert (195 von 195 Paaren aus Rolle und Tabelle). Das ist eine Probe an einer Kopie, keine Prüfung durch Dritte.

Restrisiko — eine Regel trennt die Kunden; ein Fehler in ihr beträfe alle Mandanten derselben Datenbank. Dagegen stehen die zusätzliche Regel je Tabelle, die Setzung der Kennung durch die Datenbank und die wiederholbare Probe. Wer eine harte Trennung braucht, erhält auf Wunsch eine eigene Instanz: eigene Datenbank, eigene Zugangsdaten, wahlweise im Cloud-Konto des Kunden, nach Vereinbarung. Sie besteht heute als Angebot, nicht als vorbereitete Umgebung.

— Wer hochgeladene Verträge sieht

Innerhalb eines Kunden: Administrator, Risk Manager und Freigeber sehen alle Verträge. Ein Deal Manager sieht die ihm zugeordneten, die Käuferrolle die Verträge der Käuferseite. Die Datenbank setzt das seit dem 5. August 2026 durch, auch bei direktem Zugriff auf die Schnittstelle.

Außerhalb des Kunden: Anthropic zur Analyse, siehe unten. Der Betreiber hat heute technischen Zugriff auf die Datenbank, zu Betrieb und Fehlersuche.

Gespeichert werden der aus dem Dokument gelesene Vertragstext, der Dateiname und die Analyse. Die Originaldatei wird nicht gespeichert.

Fragen an den Assistenten von CLEVER werden gespeichert und dem Betreiber einmal täglich als Liste per E-Mail zugestellt. Versanddienst ist Resend mit Sitz in den USA.

— Verarbeitung durch das Sprachmodell

Die Analyse läuft heute über die Schnittstelle von Anthropic (api.anthropic.com). Der Vertragstext wird dafür übermittelt und verlässt den Europäischen Wirtschaftsraum; die Region der Verarbeitung ist auf diesem Weg nicht auf die EU festgelegt. Grundlage sind die kommerziellen Bedingungen von Anthropic mit Auftragsverarbeitungsvereinbarung und EU-Standardvertragsklauseln. Vertragspartner für Kunden im EWR ist Anthropic Ireland, Limited (Commercial Terms of Service, Begriffsbestimmung „Anthropic“). Die Liste der Unterauftragsverarbeiter veröffentlicht Anthropic unter anthropic.com/subprocessors.

Kein Training — Anthropic trainiert nicht mit diesen Inhalten; die kommerziellen Bedingungen schließen es aus (Commercial Terms of Service, Abschnitt B). CLEVER trainiert selbst kein Modell. Der Schlüssel zur Schnittstelle liegt auf dem Server und erreicht den Browser nicht.

Aufbewahrung — Anthropic löscht Ein- und Ausgaben der Schnittstelle innerhalb von 30 Tagen, außer bei gesetzlicher Pflicht oder Verstoß gegen die Nutzungsrichtlinie (Anthropic Privacy Center, „How long do you store my organization’s data?“). Es gilt die Standard-Aufbewahrung des Anbieters; eine abweichende Vereinbarung besteht nicht.

Verarbeitung in der EU — CLEVER bietet die Analyse über Amazon Bedrock in der Region Frankfurt als buchbare Option an (Modul „Verarbeitung in der EU“, M28). Sie wird für den buchenden Kunden eingeschaltet. CLEVER selbst nutzt diesen Weg nicht, und heute läuft keine Analyse darüber. Laut Dokumentation von AWS speichert Bedrock Ein- und Ausgaben in der Voreinstellung nicht, und die Modellanbieter haben keinen Zugriff darauf. Auftragsverarbeiter ist auf diesem Weg AWS.

— Bewertungslogik und Quellcode

Die Bewertungslogik umfasst die Anweisungen an das Sprachmodell und die Risikoregister. Sie ist heute Teil der ausgelieferten Anwendung und enthält weder Kundendaten noch Zugangsschlüssel. Bei einer eigenen Instanz liegt sie serverseitig.

Der Quellcode liegt in einem privaten Repository, auf das ausschließlich der Betreiber zugreift. Ausgeliefert wird nur die gebaute Anwendung. Bei einer eigenen Instanz erhält der Kunde eine versionierte Fassung.

— Weitere Dienste

Resend versendet Benachrichtigungen von CLEVER, Absender noreply@clever-ai.org. Angemeldet wird per Anmeldelink oder mit einem Google-Konto; die Anmeldung mit einem Microsoft-Konto ist eingebaut, ihre Einrichtung für die Datenbank in Frankfurt steht noch aus. E-Mail an Personen unter clever-ai.org läuft über Microsoft 365. Ein Zahlungsdienst ist vorbereitet, aber nicht in Betrieb; er verarbeitet künftig Zahlungsdaten, keine Vertragsdaten. Die Oberfläche lädt Schriften von Google Fonts; dabei wird die IP-Adresse des Besuchers an Google übermittelt. Google Drive wird nur angesprochen, wenn ein Nutzer selbst einen Verweis auf ein dort abgelegtes Dokument einfügt.

Das Interessenformular der Startseite nimmt Einsendungen nur begrenzt an: ein unsichtbares Köderfeld, eine Mindestzeit von 2,5 Sekunden am Formular, höchstens zwei Einsendungen je Adresse und Stunde sowie fünf je Anschluss und Stunde und zwanzig je Tag, dazu eine Grenze für Verweise im Text. Die Zählung läuft im Arbeitsspeicher der Serverfunktion und ist damit kein vollständiger Schutz.

— Protokoll und Löschung

Löschungen, Wiederherstellungen, endgültige Löschungen und Compliance-Sperren werden in einem Protokoll festgehalten, das nur Einträge annimmt. Ein gelöschter Vertrag bleibt zunächst wiederherstellbar; erst die endgültige Löschung entfernt ihn samt aller Risikopositionen. Auf Wunsch entfernen wir einen Bestand vollständig.

— Was wir nicht behaupten

CLEVER ist nicht zertifiziert. Es liegt keine ISO-27001-Zertifizierung vor und keine vorgefertigte Auftragsverarbeitungsvereinbarung für Kunden. Die Trennung zwischen Kunden beruht auf einer Datenbankregel in einer gemeinsamen Datenbank; sie ist an einer Kopie geprüft, nicht durch Dritte. Getrennte Datenbanken gibt es nur als Option nach Vereinbarung, nicht als Standard.

CLEVER behauptet nicht, dass die Analyse heute in der EU läuft. Gespeichert wird in Frankfurt; analysiert wird über Anthropic außerhalb des EWR. Die Verarbeitung in der EU ist eine buchbare Option und wird erst für den Kunden eingeschaltet, der sie bucht.

Berichtigungen — die zweite Fassung dieses Dokuments nannte Frankfurt als Speicherort, als die Datenbank noch in Irland lag, und erklärte, Vertragstexte verließen den EWR nicht und würden beim Modellanbieter nicht gespeichert. Die dritte Fassung hat alle drei Angaben berichtigt. Seit dem 19. September 2026 trifft die Ortsangabe Frankfurt zu; die beiden anderen Angaben treffen für den heutigen Analyseweg weiterhin nicht zu. Die dritte Fassung nannte eine Aufbewahrung von bis zu 30 Tagen bei Anthropic als Tatsache ohne Fundstelle; die vierte Fassung kennzeichnete sie als Annahme. Seit dem 22. September 2026 ist sie mit Fundstelle belegt. Die vierte Fassung nannte getrennte Datenbanken je Kunde als Zielarchitektur und erklärte, eine Trennung per Datenbankregel gebe es nicht. Mit der Mandantentrennung in Betrieb ist es umgekehrt: Standard ist die Datenbankregel, die eigene Datenbank ist eine Option.

Fragen beantwortet Dr. Jürgen Tiedge, Geschäftsführer der Kahlstorf GmbH (CLEVER) · clever-ai.org