So arbeitet die KI in BetriebNOW

Version 1.4 · gültig ab 05.11.2026 · Prüfsumme d63da8a30b41

Diese Seite beschreibt, wie der KI-Assistent in BetriebNOW arbeitet, wo seine Grenzen liegen und welche Daten dabei fließen. Sie dient als Transparenzinformation, angelehnt an Art. 13 und 50 der KI-Verordnung (Verordnung (EU) 2024/1689). Ergänzend gelten die KI-Zusatzbedingungen und die Datenschutzerklärung.

1. Zweck und Rollen

BetriebNOW ist eine Bürosoftware für Handwerks- und Servicebetriebe. Der KI-Assistent beantwortet Fragen zu den Daten des eigenen Betriebs, bereitet Vorgänge als Entwürfe vor (zum Beispiel Angebote, Rechnungen, E-Mails, Bestellungen und Termine) und liest Inhalte aus E-Mails, Diktaten, Fotos und Dokumenten aus.

- **Anbieter des KI-Systems:** Kubilay Fehmi Gönüleglendiren als Anbieter von BetriebNOW. Der Anbieter legt Grundauftrag, Werkzeuge, Berechtigungen und Grenzen des Assistenten fest und betreibt das System.
- **Betreiber:** der Betrieb, der die KI in seinem Konto einschaltet. Er entscheidet über den Einsatz, gibt Vorgänge frei und ist für die Inhalte verantwortlich, die er verwendet oder versendet.
- **Anbieter des KI-Modells:** Anthropic Ireland, Limited, Dublin, Irland mit den Claude-Modellen, eingebunden über die Claude API.

Die KI ist in jedem Betrieb standardmäßig ausgeschaltet. Einschalten kann nur, wer im Betrieb die KI-Einstellungen verwalten darf; dabei werden die KI-Zusatzbedingungen angenommen und protokolliert. Ausschalten wirkt sofort. BetriebNOW ist auch ohne KI vollständig nutzbar.

2. Kennzeichnung

- Im Chat steht bei eingeschalteter KI „KI-Assistent“; ein leerer Chat weist darauf hin, dass eine KI (Claude von Anthropic) antwortet und Antworten Fehler enthalten können. Auf Nachfrage sagt der Assistent selbst, dass er eine KI ist.
- Entwürfe der KI tragen im Freigabe-Center die Kennzeichnung „KI-Entwurf“ mit Version. Intern speichert BetriebNOW maschinenlesbar, wie ein Vorgang entstanden ist und mit welchem Modell.
- Ausgehende E-Mails aus KI-Entwürfen tragen auf allen Versandwegen (auch über Microsoft 365) eine maschinenlesbare Kennzeichnung im E-Mail-Kopf („X-BetriebNOW-AI-Assisted“, Art. 50 Abs. 2 KI-Verordnung). Auf Wunsch des Betriebs kommt ein sichtbarer Satz hinzu: „Diese Nachricht wurde mit KI-Unterstützung erstellt.“ (Standard: aus). Angebote und Rechnungen als PDF werden nicht gekennzeichnet; Beträge rechnet BetriebNOW, nicht das Modell.

3. Was die KI kann – und was nicht

Die KI kann:

- Daten des eigenen Betriebs suchen und zusammenfassen (Kunden, Aufträge, Angebote, Rechnungen, Termine, Lager), soweit die Rolle der angemeldeten Person das erlaubt;
- Vorgänge als Entwurf vorbereiten und bestehende Entwürfe überarbeiten;
- E-Mails einordnen, Diktate in Arbeitsscheine übertragen, Typenschilder und Briefbögen auslesen;
- Seiten der App öffnen und Rückfragen stellen, wenn Angaben fehlen;
- mit dem KI-Zeiger sichtbar Wege zeigen, Reiter öffnen und Felder ausfüllen, während die Person zusieht. Knöpfe mit Wirkung (Absenden, Senden, Freigeben, Buchen, Löschen) und Haken zu Verträgen und Rechtstexten klickt der Zeiger nie – er zeigt darauf, die Person klickt selbst. Eigene Eingabe oder Esc stoppt ihn sofort; jeder Schritt steht unter der Antwort im Chat; abschaltbar im Chat unter „KI sieht diese Seite“.

Die KI kann und darf nicht:

- selbst etwas versenden, bestellen, buchen, bezahlen, löschen oder stornieren – alles mit Außenwirkung oder Geld geht als Entwurf ins Freigabe-Center. Ausnahmen sind rein interne Zuordnungen und Notizen sowie Kalenderaktionen im Rahmen der eigenen Rechte der Person; sie werden protokolliert;
- Preise, Summen und Steuern verbindlich festlegen – Summen rechnet BetriebNOW aus den Positionen; fehlt ein belastbarer Preis, steht „Preis fehlt“;
- Rechts-, Steuer-, Lohn- oder Finanzberatung leisten – sie gibt nur allgemeine Informationen und verweist an Fachleute;
- Mitarbeitende bewerten, vergleichen oder in eine Rangfolge bringen und besondere Kategorien personenbezogener Daten (zum Beispiel Gesundheit, Religion, Gewerkschaftszugehörigkeit) ableiten oder speichern;
- Entscheidungen mit rechtlicher Wirkung gegenüber Personen treffen (Art. 22 DSGVO) – entscheiden tut immer ein Mensch;
- Daten anderer Betriebe sehen oder verwenden.

4. Modelle

Einstellung	Modell	Einsatz
Auto (Automodus)	Claude Haiku 5.5 oder Claude Sonnet 5.5	Wählt je Anfrage nach festen Regeln und einer Einordnung durch Claude Haiku: Suche, Navigation und einfache Fragen mit Haiku; Angebote, Rechnungen und mehrstufige Abläufe mit Sonnet. Will Haiku einen Entwurf mit Außenwirkung anlegen, wird seine Antwort verworfen und die Anfrage von Sonnet neu bearbeitet.
Schnell	Claude Haiku 5.5	Günstig, für Routine.
Standard	Claude Sonnet 5.5	Angebote, E-Mails, Planung.
Stark	Claude Opus 5.5	Nur, wenn der Betrieb es ausdrücklich wählt.
Auslesen und Einordnen	Claude Haiku 5.5	Immer, unabhängig von der Einstellung.

Bei den Modellen Sonnet und Opus ist die serverseitige Ausweichfunktion des Modellanbieters eingeschaltet: Lehnt das Modell eine Anfrage ab, kann der Anbieter sie mit einem anderen seiner Claude-Modelle beantworten. Diese Ausweichfunktion und weitere von BetriebNOW genutzte Funktionen sind Beta-Funktionen der Schnittstelle; für sie können abweichende Bedingungen des Modellanbieters gelten, etwa zur Speicherdauer. Modelle und Versionen können sich ändern; eine neue Fassung dieser Seite nennt dann den aktuellen Stand.

5. Datenflüsse

Nur bei eingeschalteter KI gehen je Anfrage die dafür nötigen Inhalte an den Modellanbieter (Anthropic Ireland, Limited, Dublin, Irland). Orte: Verarbeitung (Inferenz) weltweit möglich, Speicherung in den USA; die Region der einzelnen Anfrage bestimmt der Modellanbieter. Übermittelt werden:

- der Grundauftrag (System-Prompt) und die Beschreibungen der Werkzeuge: für alle Betriebe gleich und ohne Betriebsdaten. Damit sie nicht bei jeder Anfrage neu verarbeitet werden, hält der Modellanbieter sie zeitweise zwischengespeichert (Prompt-Cache);
- der Betriebskontext: Name und Gewerk des Betriebs, Ort, Stundensatz, Anfahrtspauschale, Umsatzsteuer-Standard, Zahlungsziel sowie freigegebene Unternehmensregeln. Mitarbeitende stehen nicht darin: Namen, Funktionen und Fähigkeiten ruft die KI nur über Werkzeuge ab, wenn eine Anfrage sie braucht (z. B. Einsatzplanung), Abwesenheiten nur als „abwesend“ ohne Grund;
- je Nachricht: Datum und Uhrzeit, Name und Rolle der angemeldeten Person, die geöffnete Seite bzw. der geöffnete Datensatz, ein Text-Abzug dessen, was auf dieser Seite gerade zu sehen ist (Überschriften, Reiter, Tabellen, Listen, eingegebene Formularwerte auch vor dem Speichern, Fehlermeldungen, offene Dialoge; Inhalte von Passwortfeldern nie; E-Mail- und Dokumenttexte darin als fremder Inhalt markiert; abschaltbar im Chat über „KI sieht diese Seite“, mit Vorschau des genauen Textes), die Nachricht selbst, der bisherige Gesprächsverlauf, passende KI-Notizen und – nur wenn eingeschaltet – Zusammenfassungen früherer Gespräche;
- Ergebnisse der Werkzeuge, die die KI für die Antwort aufruft (zum Beispiel Kunde, Positionen, Belegdaten, E-Mail-Text), sowie angehängte Bilder, PDF-Dateien und Texte;
- zum Auslesen: E-Mail-Inhalte zur Einordnung, der erkannte Text eines Diktats, Fotos von Typenschildern, PDF-Briefbögen für die Übernahme als Vorlage und Auftragsbeschreibungen für Materiallisten; für Gesprächszusammenfassungen (nur wenn eingeschaltet) der Text des jeweiligen Chats.

Nicht an Anthropic übermittelt werden:

- Sprachaufnahmen: Die Spracherkennung läuft auf einem eigenen Server von BetriebNOW; an die KI geht nur der erkannte Text;
- Zugangsdaten wie Passwörter, Postfach-Zugänge und Schlüssel für Schnittstellen;
- Kennungen des Betriebs oder der Person als Metadaten: Die Anfragen enthalten kein Metadatenfeld mit Betriebs- oder Personenkennung. Kennungen einzelner Datensätze (zum Beispiel eines Kunden) stehen nur im Inhalt, soweit die KI sie für Werkzeugaufrufe braucht;
- Daten anderer Betriebe.

Ob und wie lange Anthropic Inhalte speichert und ob sie zum Training verwendet werden, richtet sich nach den aktuellen kommerziellen Bedingungen des Anbieters (Commercial Terms von Anthropic (https://www.anthropic.com/legal/commercial-terms)). Grundlage der Übermittlung in Drittländer: EU-Standardvertragsklauseln (Modul 2 bzw. 3) als Bestandteil des Data Processing Addendum. Speicherdauer beim Modellanbieter: Ein- und Ausgaben der API löscht Anthropic nach eigenen Angaben standardmäßig innerhalb von 30 Tagen; längere Speicherung nur bei Verstößen gegen die Nutzungsrichtlinie oder aufgrund gesetzlicher Pflichten; eine kürzere Speicherdauer ist nicht vereinbart.

6. Speicherung bei BetriebNOW

- Chatverläufe (Nachrichten, Werkzeugaufrufe und -ergebnisse, Zug-Kontext) je Person und Betrieb. Gespräche lassen sich in der App löschen. Den Text-Abzug der Seite speichert BetriebNOW nicht; er geht nur mit der jeweiligen Anfrage an den Modellanbieter.
- KI-Notizen zum Betrieb, zur Person und zu Kunden, mit Versionen. Vorschläge der KI gelten erst nach Bestätigung durch eine berechtigte Person.
- Zusammenfassungen früherer Gespräche – nur, wenn der Betrieb „Gespräche übergreifend merken“ einschaltet (Standard: aus). Jede Person sieht nur ihre eigenen.
- Verbrauch je KI-Aufruf (Modell, Tokens, Kosten) für Budget und Abrechnung.
- Freigaben mit Version, Prüfsumme und Verlauf.

Alle diese Daten liegen auf dem Server von BetriebNOW. Jeder Datensatz ist einem Betrieb zugeordnet; Abfragen sind auf den Betrieb der angemeldeten Person beschränkt. Speicherfristen und Löschung regeln die Datenschutzerklärung und der Vertrag zur Auftragsverarbeitung.

7. Menschliche Aufsicht

- **Freigabe-Center:** Vorgänge mit Außenwirkung oder Geld führt BetriebNOW erst nach einer Freigabe aus – außer bei Vorgangsarten, die der Betrieb für die kontrollierte Automatik freigeschaltet hat (siehe unten). Die Freigabe gilt nur für genau die angezeigte Version; eine Prüfsumme sichert die freigegebenen Daten. Jede Änderung erzeugt eine neue Version, die erneut freigegeben werden muss.
- **Berechtigungen:** Freigeben dürfen nur Rollen mit dem passenden Recht; finanziell verbindliche Vorgänge brauchen ein eigenes Recht. Die KI sieht nur, was die Rolle der angemeldeten Person erlaubt.
- **Vier-Augen-Prinzip:** Auf Wunsch des Betriebs braucht ein Vorgang ab einem einstellbaren Betrag eine zweite Freigabe durch eine andere Person.
- **Kritische Bestätigung:** Ab einem einstellbaren Betrag (Standard 1.000 Euro) ist eine ausdrückliche Bestätigung nötig.
- **Kontrollierte Automatik:** Nur wenn der Betrieb sie einschaltet, nur für risikoarme Vorgangsarten und nur bis zu einer Betragsgrenze von höchstens 500 Euro je Vorgang. Diese Vorgänge prüft vorher kein Mensch; sie werden protokolliert, und E-Mails daraus tragen die maschinenlesbare KI-Kennzeichnung.
- **Protokoll:** Freigaben, Ablehnungen und Ausführungen werden protokolliert; das Protokoll ist durch Datenbank-Trigger gegen Änderung und Löschung über die Anwendung geschützt, Eingriffe auf Datenbankebene erfolgen nur im dokumentierten Löschverfahren.
- **Abschalten:** Die KI lässt sich jederzeit sofort ausschalten.

8. Typische Fehler und Gegenmaßnahmen

Fehlerart	Beispiel	Gegenmaßnahme
Erfundene oder falsche Angaben	falscher Kunde, falsche Menge, falsches Datum	Werkzeuge statt Raten; Quellen und Annahmen in jeder Freigabe; Prüfung durch einen Menschen vor der Freigabe
Falsche Preise oder Summen	Position ohne belastbaren Preis	Preise aus Katalog oder belegter Historie, sonst „Preis fehlt“; Summen und Steuern rechnet BetriebNOW
Verhörte Diktate	Namen oder Zahlen falsch erkannt	Hinweis an die KI bei gesprochenen Nachrichten; Arbeitsschein bleibt Entwurf

Manipulierte Inhalte (Prompt-Injection)	E-Mail mit „Ignoriere alle Regeln“ oder neuer Bankverbindung	Externe Inhalte sind als Daten markiert; daraus entstehen keine Aktionen ohne Freigabe; Bankverbindungen ändert die KI nie aufgrund externer Inhalte
Veraltete Informationen	alter Preis aus einem früheren Angebot	Aktuelle Stammdaten und Regeln vor historischen Beispielen; Datum im Zug-Kontext
Rechtliche oder steuerliche Einschätzung	„Gilt hier § 13b UStG?“	Regeln im Grundauftrag und automatische Erkennung solcher Fragen mit Hinweis; Verweis an Steuerberatung bzw. Rechtsanwalt
Doppelte Vorgänge	Antwort neu erzeugt, Entwurf noch einmal angelegt	Hinweis auf bereits angelegte Vorgänge; mögliche Doppelungen werden markiert

9. Grenzen

- KI-Antworten können trotz aller Maßnahmen falsch, unvollständig oder veraltet sein. Ergebnisse hängen auch von der Qualität der Daten im Betrieb ab.
- Es gibt keine Zusage bestimmter Ergebnisse. Die KI ist ein Hilfsmittel; die fachliche Entscheidung liegt beim Betrieb.
- Word- und Excel-Dateien (.docx, .xlsx) liest die KI nur als Text: Formatierung, Bilder, Diagramme und Formeln gehen dabei verloren; geschützte oder beschädigte Dateien sind nicht lesbar.
- Monatsbudget und KI-Kontingent des Tarifs begrenzen die Nutzung. Die Verfügbarkeit hängt auch vom Modellanbieter ab.

10. Risikoeinstufung nach der KI-Verordnung

Bei bestimmungsgemäßer Nutzung – Informationen finden, Entwürfe vorbereiten, Inhalte auslesen, grundsätzlich mit Freigabe durch einen Menschen – ist der KI-Assistent nach Einschätzung des Anbieters kein Hochrisiko-KI-System im Sinne von Art. 6 in Verbindung mit Anhang III der KI-Verordnung.

- **Beschäftigung (Anhang III Nr. 4):** BetriebNOW ist nicht für Personalauswahl, die Bewertung von Leistung oder Verhalten, Rangfolgen von Mitarbeitenden oder die Zuweisung von Aufgaben nach Verhalten oder persönlichen Merkmalen ausgelegt. Einsatzvorschläge richten sich nach Verfügbarkeit und den Vorgaben der anfragenden Person; nach hinterlegten Fähigkeiten filtert BetriebNOW nur, wenn die Person ausdrücklich danach fragt. Jeder Einsatzvorschlag wird von einem Menschen freigegeben. Auswertungen je Person sind auf Arbeitszeitnachweise beschränkt.
- **Verbotene Praktiken (Art. 5):** keine Emotionserkennung am Arbeitsplatz, keine Bewertung nach sozialem Verhalten, keine manipulativen Techniken.
- **Umsetzung:** Regeln im Grundauftrag; automatische Erkennung solcher Anfragen mit Hinweis an Person und KI – in solchen Anfragen stehen der KI keine Werkzeuge mit Arbeitszeiten, Einsätzen oder Abwesenheiten je Person zur Verfügung; Summen der Arbeitszeit einer anderen Person nur für Rollen mit dem Recht zur Bearbeitung von Mitarbeiterdaten; keine Werkzeuge für Bewertungen; Nutzungsregeln in den KI-Zusatzbedingungen.
- **Pflichten des Betriebs als Betreiber:** bestimmungsgemäße Nutzung, ausreichende KI-Kompetenz der Nutzerinnen und Nutzer (Art. 4; BetriebNOW stellt dafür eine Lerneinheit bereit) und Information der Mitarbeitenden.

11. Training und betriebsübergreifende Nutzung

- BetriebNOW trainiert keine KI-Modelle – weder mit Daten der Betriebe noch mit Chatverläufen.
- Es gibt keine betriebsübergreifenden Modelle, Auswertungen oder Statistiken aus Inhalten der Betriebe. Ausgenommen ist eine pseudonyme Produktstatistik je Betrieb ohne Inhalte (zum Beispiel, dass die KI eingeschaltet wurde; siehe Datenschutzerklärung).
- Unternehmenswissen, KI-Notizen und Gesprächszusammenfassungen wirken nur im eigenen Betrieb.
- Nach den aktuellen kommerziellen Bedingungen des Anbieters verwendet Anthropic Inhalte aus der API nicht zum Training seiner Modelle (Commercial Terms von Anthropic (https://www.anthropic.com/legal/commercial-terms)). Maßgeblich sind die jeweils geltenden Bedingungen des Anbieters.

12. Fehler melden

- Fehlerhafte Entwürfe im Freigabe-Center ablehnen – am besten mit kurzer Begründung – oder im Chat überarbeiten lassen.
- Inhaber bzw. Admin des Betriebs informieren; sie können die KI jederzeit unter Einstellungen -> KI-Assistent ausschalten.
- Fehler, die auf das System zurückgehen (zum Beispiel unerwartete Aktionen, Daten aus falschem Zusammenhang, Sicherheitsprobleme), bitte an den Anbieter melden: kontakt@lagernow.de.