

# KI-Richtlinie für [Name des Betriebs]

Vorlage, Stand 10.10.2026  
Erklärung jeder Regel: [cyberscale.dev/ki-automatisierung/ki-richtlinie-vorlage/](https://cyberscale.dev/ki-automatisierung/ki-richtlinie-vorlage/)

Stand: [Datum] · Gilt für alle Mitarbeitenden, freien Mitarbeitenden und Praktikanten · Ansprechperson: [Name, Erreichbarkeit]

Diese Richtlinie regelt, wie wir KI-Dienste wie ChatGPT, Claude, Gemini, Copilot oder Übersetzungs- und Bildwerkzeuge im Betrieb nutzen. Sie ist bewusst kurz. Sie verbietet KI nicht, sie sagt, womit, wofür und wie.

## DIE ZEHN REGELN

- 1 Nur freigegebene Werkzeuge.** Für die Arbeit nutzen wir die Dienste aus der Werkzeugliste im Anhang, in dem dort genannten Tarif. Wer ein anderes Werkzeug braucht, fragt die Ansprechperson. Die Antwort kommt innerhalb einer Woche; bis dahin gilt: nicht nutzen.
- 2 Nur im Firmenkonto.** Angemeldet wird mit der Firmen-E-Mail-Adresse und Zwei-Faktor-Anmeldung. Private Konten, private Handy-Apps und private Abos sind für Arbeitsdaten nicht erlaubt, auch nicht „nur kurz“.
- 3 Diese Daten gibt niemand in einen KI-Dienst ein:** Namen, Adressen, Telefonnummern, Geburtsdaten, Gesundheits-, Gehalts- oder Bewerbungsdaten von Kunden, Mitarbeitenden oder Bewerbern; Zugangsdaten, Schlüssel, Passwörter; ganze Verträge, Angebote oder Rechnungen von Kunden; Kalkulationen, Lieferantenkonditionen und alles, was wir als Geschäftsgeheimnis behandeln. Ausnahme: ein Werkzeug aus der Liste, das im Anhang ausdrücklich dafür freigegeben ist. Auch dort gilt: so wenig wie nötig, Namen vorher ersetzen, wo es geht.
- 4 Training aus, Verlauf begrenzt.** In jedem freigegebenen Konto ist das Training mit unseren Eingaben abgeschaltet, soweit der Dienst den Schalter anbietet; in Geschäftstarifen ist es ohnehin aus. Chats mit Kunden- oder Betriebsbezug werden gelöscht, sobald die Aufgabe erledigt ist, spätestens nach [30] Tagen. Antworten werden nicht mit Daumen hoch oder runter bewertet, wenn fremde Daten im Chat stehen.
- 5 Ein Mensch prüft, bevor etwas nach außen geht.** Jeder Text, jede Zahl, jedes Bild aus einem KI-Dienst wird gelesen und geprüft, bevor es an Kunden, Behörden, Lieferanten oder auf die Website geht. Zahlen, Zitate, Preise, Fristen und Rechtsaussagen werden gegen die Quelle geprüft, nicht gegen eine zweite KI-Antwort. Wer das Ergebnis verschickt, steht dafür ein.
- 6 Offen sagen, wenn KI beteiligt war.** Intern antworten wir ehrlich, wenn jemand fragt, ob ein Text oder Bild mit KI entstanden ist. Nach außen kennzeichnen wir, wo das Gesetz oder der Kunde es verlangt: Ein Chatbot auf der Website sagt, dass er ein Chatbot ist; KI-erzeugte Bilder oder Stimmen echter Personen erstellen wir nicht.
- 7 Keine Entscheidungen über Menschen.** KI bewertet, sortiert oder beurteilt bei uns keine Bewerbungen, Mitarbeitenden oder Kunden und überwacht niemanden. Sie darf Vorschläge machen, die Entscheidung trifft und begründet ein Mensch. Werkzeuge, die Mitarbeitende betreffen, führen wir nur nach Abstimmung mit [Betriebsrat / der Belegschaft] ein.
- 8 Keine Erweiterungen und Agenten ohne Freigabe.** Browser-Erweiterungen mit KI, Plugins in Office-Programmen, Automatisierungen und KI-Agenten, die Mails lesen, Dateien ändern oder Nachrichten verschicken, werden nur installiert, wenn sie in der Werkzeugliste stehen. Was eigenständig handeln kann, braucht eine Freigabe je Zugriff.
- 9 Fehler sofort melden, ohne Nachteil.** Wer merkt, dass Daten im falschen Werkzeug gelandet sind, ein Konto übernommen wurde oder ein KI-Ergebnis falsch nach außen ging, meldet es am selben Tag an die Ansprechperson. Die Meldung hat keine Folgen für die meldende Person. Ob eine Datenpanne an die Datenschutzbehörde zu melden ist, entscheidet [Name] innerhalb der 72-Stunden-Frist.
- 10 Einweisung und Überprüfung.** Jede neue Mitarbeiterin und jeder neue Mitarbeiter bekommt diese Richtlinie und eine Einweisung von [30] Minuten in die freigegebenen Werkzeuge. Die Werkzeugliste prüfen wir alle [6] Monate und bei jeder Tarif- oder Anbieteränderung; das Datum der letzten Prüfung steht oben.

ANHANG: WERKZEUGLISTE

| Werkzeug        | Tarif und Konto              | Erlaubt für                                         | Nicht erlaubt für                 | Auftragsverarbeitungsvertrag | Training abgeschaltet am |
|-----------------|------------------------------|-----------------------------------------------------|-----------------------------------|------------------------------|--------------------------|
| [z. B. ChatGPT] | [Business, Firmenkonto]      | [Texte entwerfen, zusammenfassen, übersetzen, Code] | [Kundendaten, Personalunterlagen] | [ja, Datum]                  | [Datum / im Tarif aus]   |
| [z. B. DeepL]   | [Pro, Firmenkonto]           | [Übersetzungen]                                     | [Verträge ganzer Kunden]          | [ja, Datum]                  | [im Tarif aus]           |
| [z. B. Copilot] | [Arbeitskonto Microsoft 365] | [Entwürfe in Word, Outlook, Teams]                  | [Entscheidungen über Personen]    | [ja, Microsoft DPA]          | [im Tarif aus]           |
|                 |                              |                                                     |                                   |                              |                          |
|                 |                              |                                                     |                                   |                              |                          |
|                 |                              |                                                     |                                   |                              |                          |
|                 |                              |                                                     |                                   |                              |                          |

Was in die Spalten gehört: „Tarif und Konto“ ist der Geschäftstarif, auf die Firma gebucht. „Erlaubt für“ und „Nicht erlaubt für“ sind Beispiele aus eurem Alltag, keine Kategorien. „Auftragsverarbeitungsvertrag“ heißt: abgeschlossen, mit Datum abgelegt. „Training abgeschaltet am“ ist das Datum, an dem jemand den Schalter geprüft hat, oder der Hinweis, dass der Tarif gar nicht trainiert.

KENNTNISNAHME

Ich habe die KI-Richtlinie gelesen und halte sie ein.

Name

Datum

Unterschrift