EASTKAP

EU-AI-ACT-READINESS-AUDIT · MUSTER

# Muster-Report · Quick-Audit

Inventar · Risikoklassifizierung · Gap-Analyse · Maßnahmenplan

MANDANTIN (FIKTIV)
**Kontor Nord GmbH, Hamburg**
PROFIL
Online-Handel (D2C, Mode & Lifestyle) · rund 60 Mitarbeitende
ERSTELLT DURCH
Rechtsanwalt Daniel Wagner · EASTKAP, Berlin
STAND
Mai 2026

> *FIKTIVES MUSTER — veranschaulicht Aufbau und Ergebnistiefe eines EASTKAP-Audits. Keine reale Mandatsbeziehung; alle Angaben sind erfunden.*

# Inhalt

# Management Summary

Kontor Nord betreibt einen Direct-to-Consumer-Onlineshop und setzt KI an vielen Stellen ein — von der Produktempfehlung über einen Support-Chatbot und die Betrugserkennung im Checkout bis zur Vorauswahl von Bewerbungen. Das Unternehmen entwickelt selbst keine KI, ist aber als Betreiberin vom EU-AI-Act erfasst.

Das Gesamtbild ist beherrschbar, aber nicht folgenlos. Sieben KI-Systeme wurden erfasst und einzeln klassifiziert; sechs davon liegen im geringen oder begrenzten Risikobereich, eines sticht heraus: die KI-gestützte Bewerber-Vorauswahl ist ein Hochrisiko-System (Anhang III). Die strengeren Hochrisiko-Pflichten greifen nach der Digital-Omnibus-Einigung voraussichtlich erst zum 2. Dezember 2027 — die Transparenzpflichten (Art. 50) für Chatbot und KI-Inhalte jedoch bereits zum 2. August 2026, die KI-Kompetenzpflicht (Art. 4) gilt seit Februar 2025.

**Dringlichste Lücken:** kein dokumentiertes KI-Inventar, keine interne KI-Richtlinie, fehlende Schulungsnachweise (Art. 4) und Anbieterverträge ohne Auskunfts-/Dokumentationsklauseln. Hinzu kommt datenschutzrechtlicher Klärungsbedarf bei personalisierten Preisen und Profiling.

### Ampel-Gesamtbild

**AMPEL-GESAMTBILD · 8 HANDLUNGSFELDER**

| | | |
|---|---|---|
| KI-Inventar dokumentieren | ROT | sofort |
| Interne KI-Richtlinie | ROT | 4 Wochen |
| KI-Kompetenz / Schulung (Art. 4) | ROT | 6 Wochen |
| Anbieter-Klauseln (Auskunft/Doku) | ROT | Vertragsverl. |
| Transparenz Chatbot + Inhalte (Art. 50) | GELB | 02.08.2026 |
| HR-Tool als Hochrisiko vorbereiten | GELB | bis Q3 2027 |
| Personalisierte Preise / Profiling | GELB | 8 Wochen |
| Verbotene Praktiken (Art. 5) | GRÜN | keine |

*Acht Handlungsfelder nach Dringlichkeit — Rot: sofort, Gelb: terminiert, Grün: kein Handlungsbedarf.*

# 1. Auftrag, Umfang und Methodik

Gegenstand ist ein Quick-Audit der KI-Nutzung der Gesellschaft im Hinblick auf den EU-AI-Act (VO 2024/1689). Geprüft wurden alle intern eingesetzten und eingekauften KI-Systeme einschließlich einzelner Abteilungs-Accounts.

- Datengrundlage: strukturierter Fragebogen, Gespräch mit Geschäftsführung, Marketing/Shop und IT, Sichtung der eingesetzten Tools und relevanten Anbieterverträge.
- Methode: KI-augmentierte Auswertung (Klassifizierung, Abgleich mit den gesetzlichen Pflichten), jede Bewertung anwaltlich geprüft und freigegeben.
- Risikobewertung: zweidimensional nach Eintrittswahrscheinlichkeit eines Compliance-Verstoßes und Schwere (Bußgeld- und Betroffenenrisiko) — siehe Abschnitt 4.
- Nicht Gegenstand: abschließende DSGVO-Verfahrensverzeichnisse, lauterkeitsrechtliche Detailprüfung, steuerliche Fragen.

## 2. Rechtlicher Rahmen und Fristen (Stand Mai 2026)

- Verbotene Praktiken (Art. 5) und KI-Kompetenzpflicht (Art. 4): gelten seit Februar 2025.
- GPAI- und Governance-Bestimmungen: seit August 2025.
- Transparenzpflichten (Art. 50): ab 2. August 2026 — nicht verschoben.
- Hochrisiko-Pflichten (Anhang III): per Digital Omnibus (Einigung 7. Mai 2026) voraussichtlich auf 2. Dezember 2027 verschoben; formale Verabschiedung ausstehend.
- Sanktionsrahmen: bis 35 Mio. EUR / 7 % (Verbote), bis 15 Mio. EUR / 3 % (Hochrisiko- und sonstige Pflichten).

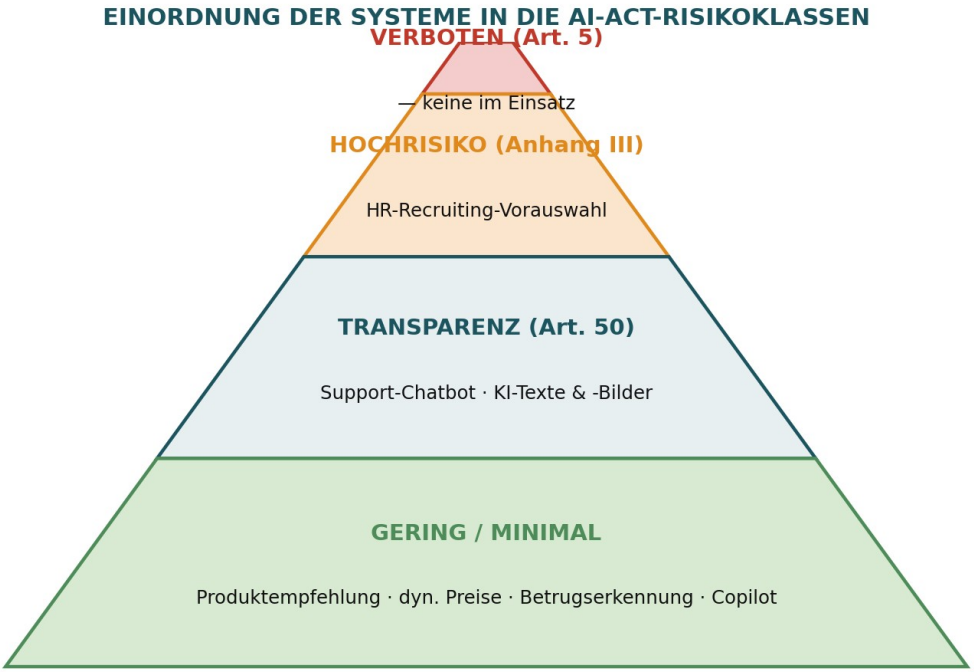

*Gestaffelte Geltung der AI-Act-Pflichten — der nächste scharfe Stichtag ist der 2. August 2026.*

## 3. KI-System-Inventar

| System | Einsatz | Anbieter (Typ) | Personenbezug |
|---|---|---|---|
| Produktempfehlung (ML) | Shop, personalisierte Empfehlungen | SaaS | ja (Kunden) |
| Support-Chatbot | Kundenservice / FAQ | SaaS | ja (Anfragen) |
| Dynamische Preisgestaltung | Preis-/Rabattsteuerung | intern/SaaS | ja (Verhalten) |
| Betrugserkennung Checkout | Zahlungs-/Bestellrisiko | Payment-/Fraud-Tool | ja (Käufer) |
| **HR-/Recruiting-Vorauswahl** | **Bewerber-Screening** | **HR-Tech-SaaS** | **ja (Bewerber)** |
| KI-Texte & -Bilder | Produkt-/Marketinginhalte | intern (GPT/Claude) | kein |
| M365 Copilot, ChatGPT | Office, Recherche | US-Anbieter | gering |

## 4. Risikoklassifizierung

Jedes System wurde zunächst der AI-Act-Risikoklasse zugeordnet (Verbot / Hochrisiko / Transparenz / gering) und anschließend nach Eintrittswahrscheinlichkeit und Schwere bewertet. Die folgende Pyramide zeigt die Einordnung im Überblick.

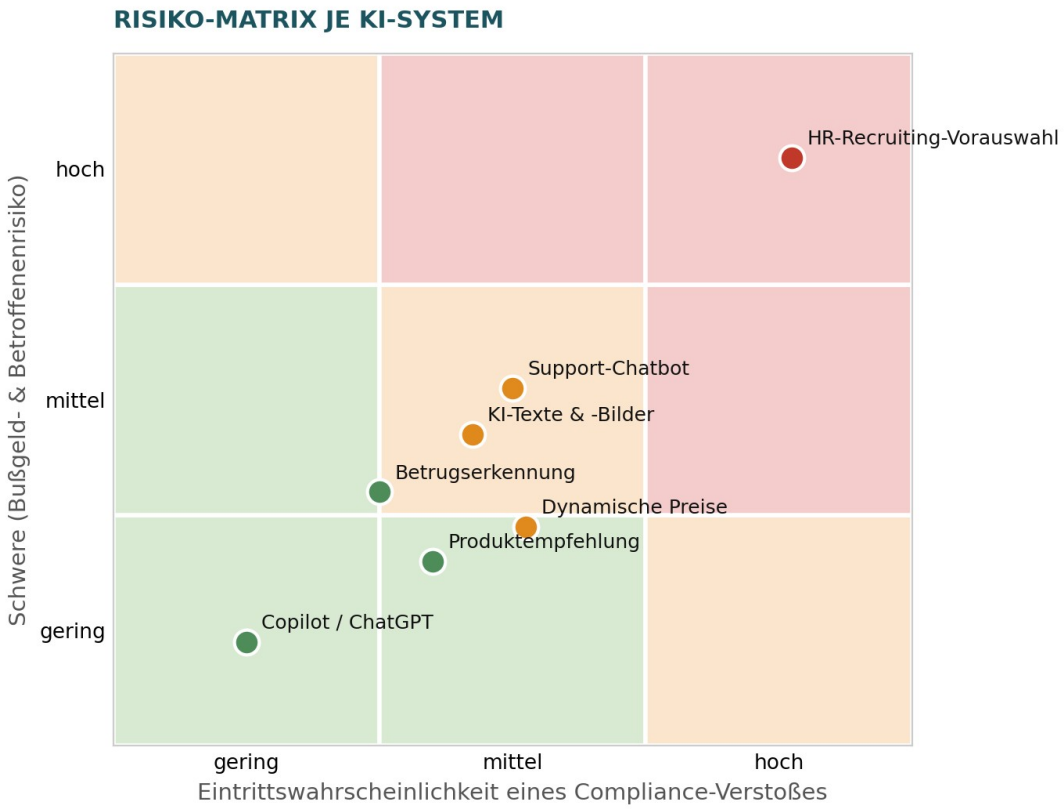



*Zuordnung der sieben Systeme zu den vier AI-Act-Risikoklassen.*

| System | Klasse | Begründung |
|---|---|---|
| **HR-/Recruiting-Vorauswahl** | **Hochrisiko (Anhang III Nr. 4)** | **KI zur Auswahl natürlicher Personen im Beschäftigungskontext — ausdrücklich als Hochrisiko gelistet.** |
| Support-Chatbot | Begrenztes Risiko (Art. 50) | Interaktion mit natürlichen Personen — Offenlegungspflicht. |
| KI-Texte & -Bilder | Begrenztes Risiko (Art. 50) | KI-erzeugte Inhalte sind als solche kenntlich zu machen. |
| Produktempfehlung | Minimal / begrenzt | Empfehlung, keine Entscheidung über Personen; DSGVO-Profiling relevant. |
| Dynamische Preisgestaltung | Minimal (AI Act) | Kein Anhang-III-Fall; relevant sind DSGVO (Profiling) und Lauterkeitsrecht. |
| Betrugserkennung Checkout | Begrenzt / minimal | Betrugsprävention; i. d. R. nicht Anhang III, Sorgfalt bei Ablehnungen. |
| Copilot, ChatGPT | Minimal | Allgemeine Produktivität; Pflichten v. a. aus Art. 4 und DSGVO. |

## 4.1 Risiko-Bewertung: Wahrscheinlichkeit × Schwere

Die Risikoklasse allein sagt wenig über die tatsächliche Dringlichkeit. Erst die Kombination aus Eintrittswahrscheinlichkeit eines Compliance-Verstoßes (wie nah ist das System an einem Verstoß, wie groß die Doku-Lücke?) und Schwere (Bußgeldrahmen, Zahl und Sensibilität der Betroffenen) ergibt das Handlungsbild.




*Risiko-Matrix: je weiter rechts oben, desto dringlicher. Die HR-Vorauswahl ist der klare Ausreißer.*

**HR-Recruiting-Vorauswahl (rot):** höchste Schwere (Hochrisiko, 15 Mio. EUR / 3 %, sensible Bewerberdaten, AGG-Bezug) bei zugleich hoher Wahrscheinlichkeit, weil das System intern als bloße Software geführt und nicht als Hochrisiko vorbereitet ist.

**Chatbot und KI-Inhalte (gelb):** mittlere Schwere, mittlere Wahrscheinlichkeit — die Transparenzpflicht (Art. 50) ist konkret und kurzfristig (02.08.2026), technisch aber einfach zu erfüllen.

**Empfehlung, Preise, Betrugserkennung, Copilot (grün):** geringe AI-Act-Schwere; der Hebel liegt hier im Datenschutz (Profiling, Art. 22 DSGVO) und in der KI-Kompetenz (Art. 4), nicht in Anhang III.

Verbotene Praktiken (Art. 5) sind nicht im Einsatz. Da die Zielgruppe auch jüngere Verbraucher umfasst, ist das Empfehlungs- und Preis-Design jedoch auf manipulative bzw. ausnutzende Muster zu prüfen (Art. 5).

## 5. Pflichten-Mapping

### 5.1 Hochrisiko (HR-Vorauswahl)

- Als Betreiberin: Nutzung gemäß Anbieter-Anleitung, wirksame menschliche Aufsicht (Art. 14), Kontrolle der Eingabedaten, Protokollaufbewahrung (Art. 12), Information der Bewerber.
- Vom Anbieter einzufordern: technische Dokumentation, Konformitätsnachweis, Registrierung — vertraglich absichern.
- Flankierend: DSGVO (Art. 22, 35), BetrVG (§§ 87, 90, 95) und AGG beachten — bei HR-KI greifen drei Regime gleichzeitig.

– Zeithorizont: Pflichten voraussichtlich ab 2. Dezember 2027; Vorbereitung jetzt.

### 5.2 Transparenz (Art. 50, ab 02.08.2026)

– Chatbot: deutlicher Hinweis, dass mit einem KI-System interagiert wird.
– KI-generierte Produktbilder/-texte: Kennzeichnung als KI-erzeugt, soweit einschlägig.

### 5.3 Querschnitt (alle Systeme)

– KI-Kompetenz (Art. 4): nachweisbare, rollengerechte Schulung aller Mitarbeitenden.
– Datenschutz: Rechtsgrundlage je Verarbeitung, Profiling-Grenzen (Art. 22 DSGVO), Transparenz, pseudonymisierter KI-Einsatz, Drittlandtransfer dokumentieren.

## 6. Gap-Analyse

| Anforderung | Soll | Ist | Bewertung |
|---|---|---|---|
| KI-Inventar dokumentiert | vorhanden | fehlt | Rot |
| Interne KI-Richtlinie | vorhanden | fehlt | Rot |
| Schulungsnachweis (Art. 4) | vorhanden | fehlt | Rot |
| Anbieter-Klauseln (Auskunft/Doku) | vereinbart | fehlt | Rot |
| Transparenzhinweise (Art. 50) | umgesetzt | teilweise | Gelb |
| HR-Tool: Hochrisiko-Vorbereitung | begonnen | offen | Gelb |
| Personalisierte Preise / Profiling | geprüft | unklar | Gelb |
| Menschliche Aufsicht HR-Tool | definiert | informell | Gelb |

## 7. Verbraucher- und Datenschutz-Besonderheiten

Im B2C-Onlinehandel verschiebt sich der Schwerpunkt vom AI Act teils zum Datenschutz- und Verbraucherrecht — beide bleiben neben dem AI Act voll anwendbar.

– Personalisierte Preise und Empfehlungen: Profiling i. S. d. Art. 22 DSGVO, Transparenz- und Informationspflichten; personalisierte Preise sind zusätzlich lauterkeitsrechtlich heikel.
– Tracking für Empfehlungen: Einwilligung nach TTDSG/Cookie-Regeln erforderlich.
– Drittland-Tools (US-KI/SaaS): Drittlandtransfer mit Rechtsgrundlage (SCC/Data Privacy Framework) dokumentieren.
– Jüngere Zielgruppen: besondere Vorsicht bei manipulativem Design (Art. 5 AI Act, Schutz Minderjähriger).

## 8. KI-Kompetenz nach Art. 4

Bei rund 60 Mitarbeitenden genügt ein schlankes, dokumentiertes Schulungskonzept:

– Basismodul für alle: Grundlagen, Grenzen, Vertraulichkeit, erlaubte/unerlaubte Nutzung (jährlich, dokumentiert).
– Vertiefung für Marketing/Shop: Umgang mit generierten Inhalten, Kennzeichnung, Halluzinations- und Bias-Erkennung.
– Verantwortliche im HR-Prozess: Aufsicht über das Vorauswahltool, Umgang mit Ergebnissen, Bewerberinformation.

## 9. Governance-Empfehlung

- Eine benannte verantwortliche Person (Geschäftsführung oder Operations) genügt bei dieser Größe — keine volle AI-Officer-Stelle nötig.
- Schlanke interne KI-Richtlinie: erlaubte Tools, Datenklassen, Pseudonymisierungspflicht, Freigabe- und Kennzeichnungsregeln.
- KI-Inventar als lebendes Dokument: halbjährliche Aktualisierung, Meldepflicht für neue Tools.
- Eskalations- und Freigabepfad für neue KI-Anwendungen vor Einführung.

## 10. Maßnahmenplan

| Maßnahme | Priorität | Frist | Verantwortlich |
|---|---|---|---|
| KI-Inventar dokumentieren, Schatten-KI einfangen | Hoch | sofort | GF |
| Interne KI-Richtlinie einführen | Hoch | 4 Wochen | GF/Operations |
| Schulung Art. 4 durchführen und dokumentieren | Hoch | 6 Wochen | Operations |
| Anbieterverträge um Auskunfts-/Doku-Klauseln ergänzen | Hoch | lfd. Verlängerung | GF/Recht |
| Transparenzhinweise Chatbot + KI-Inhalte umsetzen | Mittel | bis 02.08.2026 | Marketing/IT |
| Profiling/personalisierte Preise datenschutzrechtlich prüfen | Mittel | 8 Wochen | Datenschutz |
| HR-Tool: Hochrisiko-Pflichten vorbereiten | Mittel | bis Q3 2027 | HR/Recht |
| Menschliche Aufsicht im HR-Prozess formalisieren | Mittel | 8 Wochen | HR |

## 11. Annahmen und Hinweise

Dieser Report ist ein fiktives Muster zur Veranschaulichung. Sämtliche Angaben, Systeme und Bewertungen sind erfunden und ersetzen keine Einzelfallprüfung.

- Rechtsstand Mai 2026; die Verschiebung der Hochrisiko-Pflichten ist noch nicht final verabschiedet.
- Lauterkeits-, steuer- und vertragsrechtliche Detailfragen sind nicht abschließend Gegenstand.
- Jedes Ergebnis eines realen Audits wird durch Rechtsanwalt Daniel Wagner persönlich geprüft und freigegeben.

EASTKAP · Rechtsanwalt Daniel Wagner · Kiehlufer 9, 12059 Berlin · daniel.wagner@eastkap.de