EASTKAP

EU AI ACT READINESS AUDIT · SAMPLE

Sample Report · Quick Audit

Inventory · Risk classification · Gap analysis · Action plan

CLIENT (FICTIONAL)
Kontor Nord GmbH, Hamburg
PROFILE
Online retail (D2C, fashion & lifestyle) · approx. 60 employees
PREPARED BY
Daniel Wagner, Attorney at Law · EASTKAP, Berlin
AS OF
May 2026

> *FICTIONAL SAMPLE — illustrates the structure and depth of an EASTKAP audit. No actual client relationship; all details are invented.*

Contents

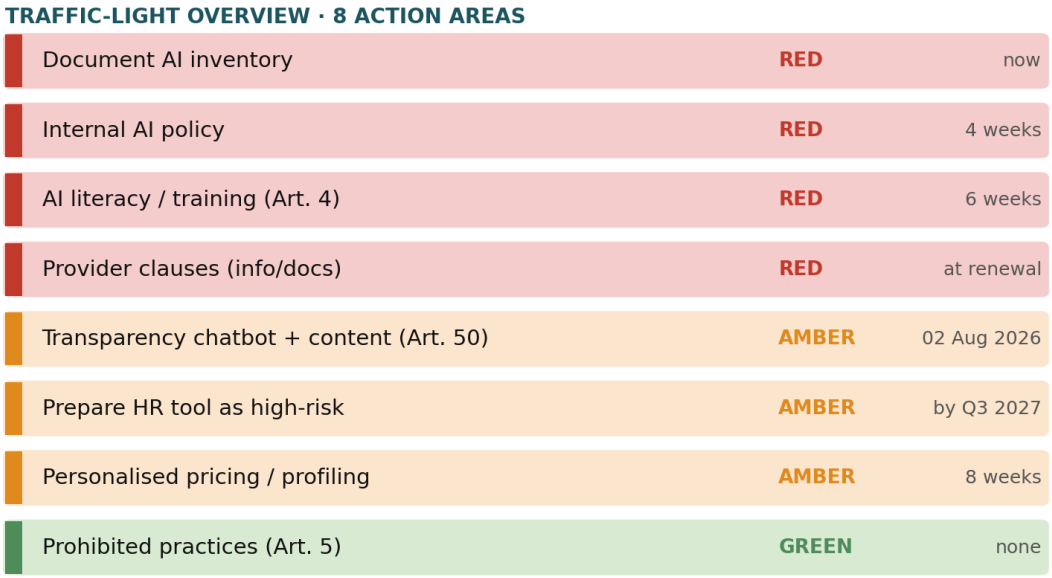
Executive Summary

Kontor Nord operates a direct-to-consumer online shop and uses AI in many places — from product recommendations and a support chatbot to fraud detection at checkout and the pre-selection of job applications. The company does not develop AI itself but, as a deployer, is covered by the EU AI Act.

The overall picture is manageable, but not without consequences. Seven AI systems were recorded and classified individually; six lie in the low or limited risk band, one stands out: the AI-assisted pre-selection of applicants is a high-risk system (Annex III). The stricter high-risk obligations apply, after the Digital Omnibus agreement, expected only from 2 December 2027 — but the transparency obligations (Art. 50) for the chatbot and AI content already from 2 August 2026, and the AI-literacy obligation (Art. 4) has applied since February 2025.

Most urgent gaps: no documented AI inventory, no internal AI policy, missing training records (Art. 4), and provider contracts without information/documentation clauses. In addition, there is a need to clarify data-protection issues around personalised pricing and profiling.

Traffic-light overview



Eight action areas by urgency — red: now, amber: scheduled, green: no action needed.

1. Engagement, scope and methodology

The subject of this engagement is a quick audit of the company's use of AI with regard to the EU AI Act (Regulation (EU) 2024/1689). All internally used and purchased AI systems were reviewed, including individual departmental accounts.

- Data basis: structured questionnaire, interviews with management, marketing/shop and IT, review of the tools in use and the relevant provider contracts.
- Method: AI-augmented analysis (classification, comparison against the statutory obligations); every assessment reviewed and approved by an attorney.
- Risk scoring: two-dimensional by likelihood of a compliance breach and severity (fine and data-subject risk) — see section 4.
- Out of scope: final GDPR records of processing, detailed unfair-competition review, tax matters.

2. Legal framework and deadlines (as of May 2026)

- Prohibited practices (Art. 5) and the AI-literacy obligation (Art. 4): in force since February 2025.
- GPAI and governance provisions: since August 2025.
- Transparency obligations (Art. 50): from 2 August 2026 — not postponed.
- High-risk obligations (Annex III): under the Digital Omnibus (agreement of 7 May 2026) expected to be postponed to 2 December 2027; formal adoption pending.
- Penalty range: up to EUR 35m / 7% (prohibitions), up to EUR 15m / 3% (high-risk and other obligations).

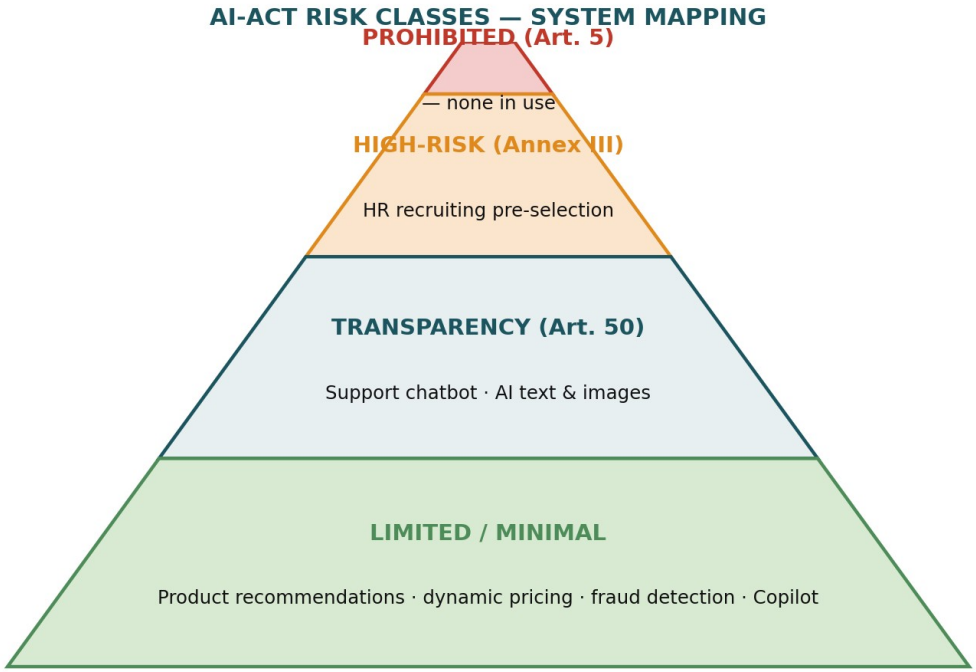
Staggered application of the AI Act obligations — the next hard deadline is 2 August 2026.

3. AI system inventory

System	Use	Provider (type)	Personal data
Product recommendations (ML)	Shop, personalised recommendations	SaaS	yes (customers)
Support chatbot	Customer service / FAQ	SaaS	yes (enquiries)
Dynamic pricing	Price/discount control	internal/SaaS	yes (behaviour)
Checkout fraud detection	Payment/order risk	Payment/fraud tool	yes (buyers)
HR / recruiting pre-selection	**Applicant screening**	**HR-tech SaaS**	**yes (applicants)**
AI text & images	Product/marketing content	internal (GPT/Claude)	none
M365 Copilot, ChatGPT	Office, research	US provider	limited

4. Risk classification

Each system was first assigned to its AI-Act risk class (prohibited / high-risk / transparency / limited) and then scored by likelihood and severity. The pyramid below shows the classification at a glance.



Mapping of the seven systems to the four AI-Act risk classes.

System	Class	Rationale
HR / recruiting pre-selection	**High-risk (Annex III No. 4)**	**AI used to select natural persons in the employment context — expressly listed as high-risk.**
Support chatbot	Limited risk (Art. 50)	Interaction with natural persons — disclosure obligation.
AI text & images	Limited risk (Art. 50)	AI-generated content must be marked as such.
Product recommendations	Minimal / limited	Recommendation, not a decision about persons; GDPR profiling relevant.
Dynamic pricing	Minimal (AI Act)	Not an Annex III case; GDPR (profiling) and unfair-competition law are relevant.
Checkout fraud detection	Limited / minimal	Fraud prevention; usually not Annex III, due care on rejections.
Copilot, ChatGPT	Minimal	General productivity; obligations mainly from Art. 4 and GDPR.

4.1 Risk scoring: likelihood × severity

The risk class alone says little about actual urgency. Only the combination of likelihood of a compliance breach (how close is the system to a breach, how large is the documentation gap?) and severity (fine range, number and sensitivity of data subjects) produces the action picture.

Risk matrix: the further top-right, the more urgent. The HR pre-selection is the clear outlier.

HR recruiting pre-selection (red): highest severity (high-risk, EUR 15m / 3%, sensitive applicant data, anti-discrimination angle) combined with high likelihood, because the system is internally treated as mere software and not prepared as high-risk.

Chatbot and AI content (amber): medium severity, medium likelihood — the transparency obligation (Art. 50) is concrete and near-term (02 Aug 2026), but technically easy to meet.

Recommendations, pricing, fraud detection, Copilot (green): low AI-Act severity; the lever here is data protection (profiling, Art. 22 GDPR) and AI literacy (Art. 4), not Annex III.

No prohibited practices (Art. 5) are in use. As the target group also includes younger consumers, the recommendation and pricing design should be reviewed for manipulative or exploitative patterns (Art. 5).

5. Obligations mapping

5.1 High-risk (HR pre-selection)

- As a deployer: use in accordance with the provider instructions, effective human oversight (Art. 14), control of input data, retention of logs (Art. 12), information to applicants.
- To be obtained from the provider: technical documentation, declaration of conformity, registration — secure contractually.
- Flanking: GDPR (Art. 22, 35), Works Constitution Act and the General Equal Treatment Act apply — HR AI triggers three regimes at once.
- Time horizon: obligations expected from 2 December 2027; prepare now.

5.2 Transparency (Art. 50, from 02 Aug 2026)

- Chatbot: clear notice that the user is interacting with an AI system.
- AI-generated product images/texts: label as AI-generated where applicable.

5.3 Cross-cutting (all systems)

- AI literacy (Art. 4): demonstrable, role-appropriate training for all staff.
- Data protection: legal basis for each processing operation, profiling limits (Art. 22 GDPR), transparency, pseudonymised AI use, document third-country transfers.

6. Gap analysis

Requirement	Target	Actual	Assessment
AI inventory documented	in place	missing	Red
Internal AI policy	in place	missing	Red
Training record (Art. 4)	in place	missing	Red
Provider clauses (info/docs)	agreed	missing	Red
Transparency notices (Art. 50)	implemented	partial	Amber
HR tool: high-risk preparation	started	open	Amber
Personalised pricing / profiling	reviewed	unclear	Amber
Human oversight HR tool	defined	informal	Amber

7. Consumer- and data-protection specifics

In B2C online retail, the focus shifts partly from the AI Act to data-protection and consumer law — both remain fully applicable alongside the AI Act.

- Personalised pricing and recommendations: profiling within the meaning of Art. 22 GDPR, transparency and information obligations; personalised pricing is additionally sensitive under unfair-competition law.
- Tracking for recommendations: consent required under the e-privacy/cookie rules.
- Third-country tools (US AI/SaaS): document third-country transfers with a legal basis (SCCs / Data Privacy Framework).
- Younger target groups: particular caution with manipulative design (Art. 5 AI Act, protection of minors).

8. AI literacy under Art. 4

With around 60 employees, a lean, documented training concept is sufficient:

- Basic module for everyone: fundamentals, limits, confidentiality, permitted/prohibited use (annual, documented).
- Deep-dive for marketing/shop: handling generated content, labelling, recognising hallucinations and bias.
- Owners of the HR process: oversight of the pre-selection tool, handling of results, applicant information.

9. Governance recommendation

- A single named responsible person (management or operations) is sufficient at this size — no full AI-officer role required.
- Lean internal AI policy: permitted tools, data classes, pseudonymisation obligation, approval and labelling rules.
- AI inventory as a living document: semi-annual update, notification obligation for new tools.
- Escalation and approval path for new AI applications before introduction.

10. Action plan

Action	Priority	Deadline	Owner
Document AI inventory, capture shadow AI	High	now	Mgmt
Introduce internal AI policy	High	4 weeks	Mgmt/Ops
Run and document Art. 4 training	High	6 weeks	Operations
Add info/documentation clauses to provider contracts	High	at renewal	Mgmt/Legal
Implement transparency notices chatbot + content	Medium	by 02 Aug 2026	Marketing/IT
Review profiling/personalised pricing (data protection)	Medium	8 weeks	Data protection
HR tool: prepare high-risk obligations	Medium	by Q3 2027	HR/Legal
Formalise human oversight in the HR process	Medium	8 weeks	HR

11. Assumptions and notes

This report is a fictional sample for illustration. All details, systems and assessments are invented and do not replace a case-by-case review.

- Legal position as of May 2026; the postponement of the high-risk obligations has not yet been formally adopted.
- Detailed questions of unfair-competition, tax and contract law are not conclusively covered.
- The result of any real audit is reviewed and approved personally by Daniel Wagner, Attorney at Law.

EASTKAP · Daniel Wagner, Attorney at Law · Kiehlufer 9, 12059 Berlin, Germany · daniel.wagner@eastkap.de