Musterbericht (echtes Analyse-Ergebnis)

Risikoklassifizierung (3)

TalentMatch - automatisierte Vorauswahl/Bewertung von Bewerbungen mit Auto-Ablehnung bei Score < 30 - Hochrisiko-KI-System
Fällt unter Anhang III Nr. 4 lit. a (Sichten/Filtern/Bewerten von Bewerbungen). Die Ausnahme nach Art. 6 Abs. 3 ist gesperrt, da das System Profiling natürlicher Personen vornimmt und eine abgeschlossene menschliche Bewertung vollständig ersetzt (automatische Ablehnung ohne Prüfung).
Norm: Art. 6 Abs. 2 i. V. m. Anhang III Nr. 4 lit. a AI Act; Sperrung der Ausnahme gem. Art. 6 Abs. 3 UAbs. 2 AI Act

Fotoverarbeitung innerhalb TalentMatch (unklare Funktion) - unklar
Es ist nicht dokumentiert, ob aus Fotos Emotionen abgeleitet oder biometrische Kategorisierung nach sensiblen Merkmalen vorgenommen wird. Falls ja, würde dies eine verbotene Praxis nach Art. 5 darstellen.
Norm: Art. 5 Abs. 1 lit. f bzw. lit. g AI Act

Basis-LLM des US-Anbieters (GPAI-Modell) - KI-Modell mit allgemeinem Verwendungszweck (GPAI)
Ursprüngliches Basismodell ist ein GPAI-Modell; Pflichten treffen originär den US-Anbieter. Durch Fine-Tuning für einen Hochrisiko-Zweck können zusätzliche Pflichten für das anpassende Unternehmen entstehen (Art. 25).
Norm: Art. 51 ff., Art. 53 AI Act; Art. 25 Abs. 1 lit. c AI Act

Anforderungen (nach Frist sortiert) (13)

[EU AI Act] Art. 4 AI Act - nicht erfüllt (Frist: gilt seit 02.02.2025 - überfällig)
KI-Kompetenz des mit Betrieb/Nutzung befassten Personals sicherstellen

Keine Schulungsnachweise vorhanden.
Norm: Art. 4 AI Act

[EU AI Act] Art. 5 Abs. 1 lit. f, lit. g AI Act - unklar / nicht dokumentiert (Frist: gilt seit 02.02.2025 - überfällig)
Prüfung, ob Fotoverarbeitung eine verbotene Praxis (Emotionserkennung/biometrische Kategorisierung) darstellt

Zweck der Fotoverarbeitung ist nicht dokumentiert.
Norm: Art. 5 Abs. 1 lit. f, lit. g AI Act

[DSGVO] Art. 22 DSGVO - nicht erfüllt (Frist: gilt bereits)
Schutz vor ausschließlich automatisierten Entscheidungen mit rechtlicher Wirkung

Automatische Ablehnung ohne Menschen, keine dokumentierten Garantien nach Art. 22 Abs. 3.
Norm: Art. 22 DSGVO

[DSGVO] Art. 35 DSGVO - nicht erfüllt (Frist: gilt bereits)
Durchführung einer Datenschutz-Folgenabschätzung

Explizit als fehlend dokumentiert; systematische automatisierte Bewertung mit Rechtswirkung erfordert DSFA.
Norm: Art. 35 DSGVO

[DSGVO] Art. 9 DSGVO - unklar / nicht dokumentiert (Frist: gilt bereits)
Rechtsgrundlage für Verarbeitung ggf. besonderer Kategorien personenbezogener Daten (Fotos)

Keine Angabe zur Rechtsgrundlage der Fotoverarbeitung.

Norm: Art. 9 DSGVO

[EU AI Act] Art. 25 Abs. 1 lit. c AI Act - nicht erfüllt (Frist: in 27 Tagen (02.08.2026))
Klärung und Dokumentation des Rollenwechsels zum Anbieter durch Zweckänderung via Fine-Tuning

Keine Dokumentation zur Rollenbestimmung oder Kooperation mit dem Erstanbieter vorhanden.
Norm: Art. 25 Abs. 1 lit. c AI Act

[EU AI Act] Art. 9 AI Act - nicht erfüllt (Frist: in 27 Tagen (02.08.2026))
Einrichtung eines Risikomanagementsystems für das Hochrisiko-KI-System

Kein Risikomanagement-Dokument vorhanden.
Norm: Art. 9 AI Act

[EU AI Act] Art. 10 AI Act - nicht erfüllt (Frist: in 27 Tagen (02.08.2026))
Daten-Governance inkl. Bias-Prüfung der Trainingsdaten

Keine Angaben zu Datenqualität, Repräsentativität oder Bias-Tests der historischen Bewerbungsdaten.
Norm: Art. 10 AI Act

[EU AI Act] Art. 13 AI Act - nicht erfüllt (Frist: in 27 Tagen (02.08.2026))
Erstellung einer Betriebsanleitung für Betreiber/Recruiter

Explizit als fehlend dokumentiert.
Norm: Art. 13 AI Act

[EU AI Act] Art. 14 AI Act - nicht erfüllt (Frist: in 27 Tagen (02.08.2026))
Gewährleistung wirksamer menschlicher Aufsicht

Automatische Ablehnung bei Score < 30 ohne jede menschliche Prüfung widerspricht Art. 14 Abs. 4.
Norm: Art. 14 AI Act

[EU AI Act] Art. 26 Abs. 7 AI Act - nicht erfüllt (Frist: in 27 Tagen (02.08.2026))
Information der Arbeitnehmervertreter und betroffenen Beschäftigten vor Inbetriebnahme

Betriebsrat wurde explizit nicht informiert.
Norm: Art. 26 Abs. 7 AI Act

[EU AI Act] Art. 27 AI Act - nicht erfüllt (aber nicht einschlägig)
Grundrechte-Folgenabschätzung

Private Betreiber ohne öffentlichen Dienstleistungsbezug und ohne Bezug zu Anhang III Nr. 5 lit. b/c sind von Art. 27 nicht erfasst; keine FRIA-Pflicht.
Norm: Art. 27 AI Act

[DORA] Art. 5 ff., Art. 28 DORA - unklar / nicht dokumentiert (Frist: Datum offen)
IKT-Risikomanagement/Drittparteirisiko

Kein Hinweis, dass Auftraggeber Finanzunternehmen ist; DORA erscheint nicht einschlägig.
Norm: Art. 5 ff., Art. 28 DORA

Risiken (7)

[EU AI Act] Diskriminierung durch Bias in historischen Trainingsdaten (z. B. Gender, Herkunft)
Eintrittswahrscheinlichkeit: hoch · Schwere: hoch

Norm: Art. 10 Abs. 2 lit. f AI Act

[DSGVO] Automatisierte Ablehnung ohne menschliche Kontrolle verletzt Recht auf menschliches Eingreifen
Eintrittswahrscheinlichkeit: hoch · Schwere: hoch
Norm: Art. 22 DSGVO

[EU AI Act] Mögliche verbotene Praxis, falls Fotoverarbeitung Emotionserkennung/biometrische Kategorisierung umfasst
Eintrittswahrscheinlichkeit: mittel · Schwere: hoch
Norm: Art. 5 Abs. 1 lit. f, lit. g AI Act

[DSGVO] Fehlende DSFA trotz systematischer automatisierter Bewertung mit Rechtswirkung
Eintrittswahrscheinlichkeit: hoch · Schwere: hoch
Norm: Art. 35 DSGVO

[EU AI Act] Bußgeld- und Haftungsrisiko wegen Nichterfüllung der Hochrisiko-Pflichten ab 02.08.2026
Eintrittswahrscheinlichkeit: hoch · Schwere: hoch
Norm: Art. 9 bis Art. 15, Art. 26 AI Act

[EU AI Act] Mitbestimmungsverstoß durch fehlende Betriebsratsinformation
Eintrittswahrscheinlichkeit: hoch · Schwere: mittel
Norm: Art. 26 Abs. 7 AI Act

[Sonstiges] Reputationsschaden bei Bekanntwerden vollautomatisierter Ablehnungen ohne Kontrolle
Eintrittswahrscheinlichkeit: mittel · Schwere: hoch
Norm: keine spezifische Norm - reputationsbezogenes Risiko
! Normverweis: außerhalb des Korpus (nicht geprüft)

Regelungslücken (8)

[EU AI Act] Kein Risikomanagement-Dokument
Fehlt: Risikoidentifikation, -bewertung und -minderungsmaßnahmen gemäß Art. 9

Relevanz: Pflicht ab 02.08.2026 zwingend für Hochrisiko-KI-Systeme

[DSGVO] Keine Datenschutz-Folgenabschätzung
Fehlt: Systematische Bewertung der Risiken für Rechte und Freiheiten Betroffener

Relevanz: Zwingend erforderlich bei automatisierter Bewertung mit Rechtswirkung (Art. 35 Abs. 3 lit. a)

[EU AI Act] Keine Betriebsanleitung für Recruiter
Fehlt: Informationen zu Leistungsgrenzen, Genauigkeit, menschlicher Aufsicht

Relevanz: Pflicht des Anbieters nach Art. 13 zur ordnungsgemäßen Nutzung durch Betreiber

[EU AI Act] Keine Schulungsnachweise
Fehlt: Nachweis ausreichender KI-Kompetenz des Personals

Relevanz: Bereits seit 02.02.2025 geltende Pflicht nach Art. 4

[EU AI Act] Keine Information des Betriebsrats
Fehlt: Nachweis der Unterrichtung von Arbeitnehmervertretern vor Inbetriebnahme

Relevanz: Art. 26 Abs. 7 und BetrVG-Mitbestimmung

[EU AI Act] Zweck der Fotoverarbeitung ungeklärt
Fehlt: Konkrete Funktion/Verwendung der Fotos im Scoring-Prozess

Relevanz: Mögliche verbotene Praxis nach Art. 5, falls Emotions-/Biometrieerkennung vorliegt

[EU AI Act] Keine vertragliche Vereinbarung mit US-Basismodell-Anbieter dokumentiert
Fehlt: Informationsfluss, technischer Zugang, Unterstützung gemäß Art. 25 Abs. 4

Relevanz: Erforderlich zur Erfüllung der Anbieterpflichten bei Rollenwechsel

[DSGVO] Unklare internationale Datenübermittlung an US-Anbieter
Fehlt: Nachweis über Datenflüsse, Standardvertragsklauseln o. ä.

Relevanz: Kapitel V DSGVO bei Beteiligung eines US-Anbieters trotz EU-Hosting

Maßnahmen (nach Priorität) (10)

[DSGVO] Sofortige Einführung menschlicher Überprüfung vor jeder automatischen Ablehnung
Priorität: hoch · Norm/Grundlage: Art. 22 DSGVO
Norm: Art. 22 DSGVO

[EU AI Act] Klärung der Fotoverarbeitung und ggf. Aussetzung bis Klärung erfolgt
Priorität: hoch · Norm/Grundlage: Art. 5 AI Act
Norm: Art. 5 AI Act

[EU AI Act] Durchführung Schulungen zur KI-Kompetenz und Dokumentation der Nachweise
Priorität: hoch · Norm/Grundlage: Art. 4 AI Act
Norm: Art. 4 AI Act

[DSGVO] Durchführung einer Datenschutz-Folgenabschätzung
Priorität: hoch · Norm/Grundlage: Art. 35 DSGVO
Norm: Art. 35 DSGVO

[EU AI Act] Information und Beteiligung des Betriebsrats vor weiterem Einsatz
Priorität: hoch · Norm/Grundlage: Art. 26 Abs. 7 AI Act
Norm: Art. 26 Abs. 7 AI Act

[EU AI Act] Aufbau eines Risikomanagementsystems inkl. Bias-Testung der Trainingsdaten
Priorität: hoch · Norm/Grundlage: Art. 9, Art. 10 AI Act
Norm: Art. 9, Art. 10 AI Act

[EU AI Act] Erstellung von Betriebsanleitung, technischer Dokumentation und Logging-Konzept
Priorität: hoch · Norm/Grundlage: Art. 11-13 AI Act
Norm: Art. 11-13 AI Act

[EU AI Act] Klärung und Dokumentation der Anbieterrolle nach Art. 25 sowie Abstimmung mit US-Basismodell-Anbieter
Priorität: hoch · Norm/Grundlage: Art. 25 AI Act
Norm: Art. 25 AI Act

[EU AI Act] Vorbereitung Konformitätsbewertung, CE-Kennzeichnung und Registrierung vor 02.08.2026

Priorität: hoch · Norm/Grundlage: Art. 43, 48, 49 AI Act
Norm: Art. 43, 48, 49 AI Act

[DSGVO] Klärung internationaler Datenübermittlungen an US-Anbieter und Absicherung nach Kapitel V DSGVO
Priorität: mittel · Norm/Grundlage: Kapitel V DSGVO
Norm: Kapitel V DSGVO
! Normverweis: außerhalb des Korpus (nicht geprüft)

Ausführlicher Bericht

Compliance-Analyse: KI-System "TalentMatch"

Prüfdatum: 2026-07-05 - Hinweis: Zu diesem Zeitpunkt gelten Kapitel I/II (Art. 4, Art. 5) bereits seit 02.02.2025 sowie Kapitel V/VII/XII seit 02.08.2025. Die Hochrisiko-Pflichten (Art. 8-27) treten erst am **02.08.2026** in Kraft - das ist **weniger als 4 Wochen nach dem Prüfdatum**. Angesichts dieser unmittelbaren Frist ist eine "gilt demnächst"-Einordnung hier faktisch als **akuter Handlungsbedarf** zu behandeln.

---

1. Systembeschreibung, Einsatzkontext und Rollenbestimmung (inkl. Art. 25)

System: "TalentMatch" - automatisierte Vorauswahl von Bewerbungen mittels feinabgestimmtem LLM; Score 0-100; automatische Ablehnung bei Score < 30 **ohne menschliche Prüfung** (systembeschreibung.txt).

Betroffene Personen: Bewerberinnen/Bewerber; verarbeitete Daten: Name, Lebenslauf, Anschreiben, teilweise Fotos (systembeschreibung.txt).

Modellherkunft: Fine-Tuning eines Basis-LLM eines US-Anbieters, Hosting in der EU, Fine-Tuning durch das Unternehmen selbst mit historischen Bewerbungsdaten (systembeschreibung.txt).

Rollenbestimmung - Art. 25 AI Act (zentraler Befund):
Das Basismodell (GPAI, US-Anbieter) war ursprünglich nicht als Hochrisiko-System eingestuft. Durch das eigenständige Fine-Tuning für den **spezifischen Zweck der Bewerberauswahl** hat das Unternehmen die Zweckbestimmung des KI-Systems so verändert, dass es zu einem Hochrisiko-KI-System im Sinne von Art. 6 wird (Anhang III Nr. 4 lit. a). Dies entspricht exakt dem Tatbestand des **Art. 25 Abs. 1 lit. c**: Wer die Zweckbestimmung eines KI-Systems (einschließlich GPAI) so verändert, dass es hochriskant wird, **wird selbst zum Anbieter** mit sämtlichen Anbieterpflichten. Das Unternehmen ist damit **nicht nur Betreiber, sondern zugleich Anbieter** dieses konkreten Systems - der im Auftrag beschriebene Standardfall bei KMU, die Basismodelle anpassen.

Konsequenz: Das Unternehmen trägt kumulativ:
- Anbieterpflichten (Art. 9-15, 43, 48, 49 - analog zu Art. 16, sofern anwendbar)
- Betreiberpflichten (Art. 26), da es das System auch selbst im eigenen Recruiting einsetzt.

Der ursprüngliche US-Anbieter des Basismodells bleibt gemäß Art. 25 Abs. 2 zur Kooperation und Informationsbereitstellung verpflichtet, sofern er die Weiterverwendung nicht ausgeschlossen hat - dies ist aus den Unterlagen nicht erkennbar (Regelungslücke).

---

2. Risikoklassifizierung nach EU AI Act (inkl. Prüfung Art. 5 und Art. 6 Abs. 3)

a) Verbotene Praktiken (Art. 5):
Keine der Unterlagen belegt eine der Tatbestände abschließend als erfüllt. **Aber:** Die Verarbeitung von Bewerberfotos ist ungeklärt. Sollte das System aus Fotos Emotionen ableiten oder biometrische Kategorisierung nach sensiblen Merkmalen vornehmen, wäre dies am Arbeitsplatz-Bewerbungskontext **unmittelbar von Art. 5 Abs. 1 lit. f bzw. lit. g erfasst und verboten** (keine medizinische/Sicherheits-Ausnahme einschlägig). Dies ist als **kritische, umgehend zu klärende offene Frage** auszuweisen (systembeschreibung.txt: "teilweise Fotos", ohne Zweckangabe).

b) Hochrisiko nach Art. 6 Abs. 2 i. V. m. Anhang III:
Das System fällt eindeutig unter **Anhang III Nr. 4 lit. a** ("KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, ... um Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten"). Damit ist TalentMatch ein **Hochrisiko-KI-System**.

c) Ausnahme nach Art. 6 Abs. 3:
Zu prüfen wäre, ob eine der Ausnahmen (lit. a-d) greift. Das System trifft jedoch eine **abschließende automatisierte Entscheidung ohne menschliche Prüfung** bei Score < 30 - dies ist keine "eng gefasste Verfahrensaufgabe", keine bloße Verbesserung einer abgeschlossenen menschlichen Tätigkeit und keine reine Abweichungserkennung, sondern **ersetzt die menschliche Bewertung vollständig**. Zudem nimmt das System **Profiling natürlicher Personen** vor (Bewertung von Personen anhand abgeleiteter Merkmale aus Lebenslauf/Anschreiben/Foto). Gemäß Art. 6 Abs. 3 Unterabsatz 2 ist die Ausnahme damit **gesperrt** - das System gilt **zwingend als hochriskant**. Eine Dokumentation nach Art. 6 Abs. 4 liegt ohnehin nicht vor und wäre wegen des Profilings auch unbeachtlich.

d) Transparenzpflichten (Art. 50): Einschlägig, sobald das System als Chatbot mit direkter Interaktion fungieren würde - aus den Unterlagen nicht ersichtlich; primär relevant wäre Art. 50 Abs. 3, falls Emotionserkennung/biometrische Kategorisierung vorliegt (s. o.).

e) GPAI: Das Basismodell selbst ist ein GPAI-Modell eines US-Anbieters; die Pflichten aus Art. 53 ff. treffen originär diesen Anbieter, ggf. aber auch das Unternehmen als Anbieter des abgeleiteten Systems, sofern es das Basismodell wesentlich verändert hat (nicht abschließend klärbar aus den Unterlagen).

Ergebnis: **Hochrisiko-KI-System** nach Art. 6 Abs. 2 i. V. m. Anhang III Nr. 4 lit. a - Ausnahme gesperrt wegen Profiling.

---

3. Bereits geltende Pflichten: KI-Kompetenz (Art. 4) und ggf. Verbote (Art. 5)

- **Art. 4 (KI-Kompetenz, gilt seit 02.02.2025):** Es liegen **keine Schulungsnachweise** vor (systembeschreibung.txt). Dies ist eine **bereits jetzt bestehende, verletzte Pflicht** - sowohl in der Anbieter- als auch in der Betreiberrolle.
- **Art. 5 (Verbote, gilt seit 02.02.2025):** Kein gesicherter Verstoß feststellbar, aber die ungeklärte Fotonutzung stellt ein **erhebliches Risiko einer verbotenen Praxis** dar und muss vorrangig geklärt werden, bevor das System weiterbetrieben wird.

---

4. Pflichten für Hochrisiko-KI-Systeme (ab 02.08.2026 - unmittelbar bevorstehend)

Pflicht Status
Risikomanagementsystem (Art. 9) **Nicht erfüllt** - kein Dokument vorhanden
Daten-Governance (Art. 10), insb. Bias-Prüfung bei Trainingsdaten aus historischen Bewerbungen **Nicht erfüllt/nicht dokumentiert** - erhebliches Diskriminierungsrisiko, da historische Bewerbungsdaten typischerweise bestehende Verzerrungen (Gender, Herkunft) reproduzieren
Technische Dokumentation (Art. 11, Anhang IV) Nicht dokumentiert
Aufzeichnungspflichten/Logging (Art. 12) Unklar/nicht dokumentiert
Transparenz gegenüber Betreibern (Art. 13, Betriebsanleitung) **Nicht erfüllt** - explizit als fehlend genannt
Menschliche Aufsicht (Art. 14) **Nicht erfüllt** - automatische Ablehnung ohne Menschen widerspricht Art. 14 Abs. 4 lit. d/e unmittelbar
Genauigkeit/Robustheit/Cybersicherheit (Art. 15) Nicht dokumentiert
Konformitätsbewertung/CE (Art. 43, 48) Nicht dokumentiert
Registrierung (Art. 49) Nicht dokumentiert
Betreiberpflichten (Art. 26): bestimmungsgemäße Verwendung, geschultes Personal, Überwachung Nicht erfüllt/nicht dokumentiert
Art. 26 Abs. 7 - Information der Arbeitnehmervertreter/Beschäftigten **Explizit nicht erfüllt** - "Betriebsrat wurde nicht informiert"

Da diese Pflichten erst ab 02.08.2026 rechtlich verbindlich werden, aber der Prüfzeitpunkt nur wenige Tage davor

liegt, besteht **akuter Umsetzungsdruck**; ein Weiterbetrieb ohne Nachbesserung ab dem Stichtag wäre rechtswidrig.

---

5. Transparenz- und GPAI-Pflichten (falls einschlägig)

- **Art. 50 Abs. 1/3:** Sollte das System direkt mit Bewerbern interagieren (z. B. Chat-Vorauswahl) oder Emotions-/biometrische Kategorisierung vornehmen, wären Informationspflichten ab 02.08.2026 einschlägig. Aus den Unterlagen nicht abschließend klärbar.
- **Art. 53 (GPAI):** Trifft grundsätzlich den US-Basismodell-Anbieter; ob durch das Fine-Tuning eigene GPAI-Pflichten für das Unternehmen entstehen, ist nicht dokumentiert (Regelungslücke, insb. zur Frage der "wesentlichen Veränderung" des Modells).

---

6. Grundrechte-Folgenabschätzung Art. 27 (Einschlägigkeit ausdrücklich prüfen)

Art. 27 gilt nur für: (i) Einrichtungen des öffentlichen Rechts, (ii) private Erbringer öffentlicher Dienste, (iii) Betreiber nach Anhang III Nr. 5 lit. b/c (Kreditwürdigkeit, Versicherungsrisiko). Das vorliegende System fällt unter **Anhang III Nr. 4 (Beschäftigung)**, nicht unter Nr. 5 lit. b/c. Das Unternehmen ist ein privater Arbeitgeber ohne erkennbaren öffentlichen Dienstleistungsbezug.

Ergebnis: Art. 27 FRIA ist NICHT einschlägig. Es sollte daher keine FRIA gefordert werden. Stattdessen besteht eine **DSFA-Pflicht nach Art. 35 DSGVO** (s. Abschnitt 7), die hier ersatzweise die relevante Folgenabschätzung darstellt.

---

7. Datenschutzrechtliche Bewertung nach DSGVO

- **Rechtsgrundlage (Art. 6 DSGVO):** Nicht dokumentiert, welche Rechtsgrundlage für Fine-Tuning mit historischen Bewerbungsdaten und für die laufende Bewertung neuer Bewerbungen herangezogen wird.
- **Art. 22 DSGVO (automatisierte Entscheidung):** Die automatische Ablehnung bei Score < 30 **ohne menschliche Prüfung** ist eine ausschließlich automatisierte Entscheidung mit rechtlicher/ähnlich erheblicher Wirkung (Verlust der Bewerbungschance) im Sinne von Art. 22 Abs. 1. Es liegt **kein Nachweis vor**, dass eine Ausnahme nach Art. 22 Abs. 2 greift (z. B. Vertragserforderlichkeit ist im Einstellungsverfahren rechtlich umstritten) noch dass die nach Art. 22 Abs. 3 zwingenden Mindestgarantien (Recht auf menschliches Eingreifen, Darlegung des Standpunkts, Anfechtung) implementiert sind. **Dies ist ein gravierender Verstoß.**
- **Art. 9 DSGVO:** Foto-Verarbeitung kann besondere Kategorien personenbezogener Daten offenlegen (ethnische Herkunft, Religion, Gesundheit). Ohne Zweckklärung besteht ein **ungeklärtes Risiko unrechtmäßiger Verarbeitung sensibler Daten**.
- **Art. 35 DSGVO (DSFA):** Angesichts systematischer automatisierter Bewertung mit Rechtswirkung (Art. 35 Abs. 3 lit. a) ist eine DSFA **zwingend erforderlich**. Sie liegt laut Unterlagen **nicht vor** - klare Regelungslücke.
- **Kapitel V DSGVO (internationale Übermittlung):** Basismodell stammt von US-Anbieter; obwohl Hosting in der EU erfolgt, ist unklar, ob Daten (z. B. für API-Zugriffe, Support, Modellwartung) in die USA übermittelt werden. Ungeklärt - nachzufordern.

---

8. DORA-Bezug

Nicht einschlägig. Aus den Unterlagen ergibt sich kein Hinweis, dass das Unternehmen ein Finanzunternehmen ist oder als IKT-Drittdienstleister für den Finanzsektor fungiert. Ein DORA-Bezug wird daher nicht angenommen; sollte sich der Auftraggeber doch im Finanzsektor bewegen, wäre dies nachzuliefern.

---

9. Governance, menschliche Aufsicht und Beschäftigteninformation (Art. 26 Abs. 7)

- **Menschliche Aufsicht:** Faktisch nicht vorhanden - die automatische Ablehnung erfolgt ohne jede menschliche

Beteiligung, was sowohl Art. 14 (Anbieterpflicht zur Ausgestaltung) als auch Art. 22 DSGVO widerspricht.
- **Beschäftigteninformation (Art. 26 Abs. 7):** **Explizit nicht erfüllt** - der Betriebsrat wurde nicht informiert. Dies ist zugleich ein mitbestimmungsrechtliches Risiko nach BetrVG (unabhängig vom AI Act bereits jetzt regelmäßig relevant, spätestens ab Inbetriebnahme des Hochrisiko-Systems zwingend vorgeschrieben).
- **Eskalationswege/Meldepflichten (Art. 73):** Nicht dokumentiert.

---

10. Technische Robustheit, Genauigkeit und Cybersicherheit

Keine Angaben zu Testverfahren, Genauigkeitsmetriken, Bias-Tests oder Cybersicherheitsmaßnahmen (Art. 15) in den Unterlagen. Angesichts der Verwendung historischer Bewerbungsdaten für das Fine-Tuning besteht ein **erhöhtes Risiko der Reproduktion diskriminierender Muster** (z. B. Gender-/Herkunftsbias), das nicht durch dokumentierte Gegenmaßnahmen (Art. 10 Abs. 2 lit. f/g) adressiert wird.

---

11. Risikobeurteilung

Risiko Eintrittswahrscheinlichkeit Schwere
Diskriminierung durch Bias in Trainingsdaten hoch hoch
Verstoß gegen Art. 22 DSGVO (keine menschliche Kontrolle bei Ablehnung) hoch hoch
Mögliche verbotene Praxis bei Fotoverarbeitung (Emotion/Biometrie) unklar (mittel) sehr hoch, falls zutreffend
Fehlende DSFA / Rechtsgrundlage für Verarbeitung besonderer Datenkategorien hoch hoch
Bußgeldrisiko AI Act (Hochrisiko-Pflichtverletzung ab 02.08.2026) hoch hoch
Mitbestimmungsverstoß (fehlende Betriebsratsinformation) hoch mittel
Reputationsschaden bei Bekanntwerden automatisierter Ablehnungen ohne Kontrolle mittel hoch

---

12. Regelungslücken und fehlende Nachweise

1. **Fehlendes Risikomanagementsystem** (Art. 9) - keine Dokumentation vorhanden.
2. **Fehlende DSFA** (Art. 35 DSGVO) - zwingend erforderlich, nicht durchgeführt.
3. **Fehlende Betriebsanleitung** (Art. 13) für Recruiter.
4. **Fehlende Schulungsnachweise** (Art. 4) - bereits jetzt geltende Pflicht verletzt.
5. **Fehlende Information des Betriebsrats** (Art. 26 Abs. 7 / BetrVG).
6. **Ungeklärter Zweck der Fotoverarbeitung** - Risiko einer verbotenen Praxis (Art. 5 Abs. 1 lit. f/g).
7. **Fehlende vertragliche Vereinbarung mit dem US-Basismodell-Anbieter** nach Art. 25 Abs. 4 (Informationsfluss, technischer Zugang zur Erfüllung der Anbieterpflichten).
8. **Ungeklärte internationale Datenübermittlung** (Kapitel V DSGVO) trotz EU-Hosting.
9. **Keine Nachweise zu Bias-Tests/Genauigkeits- und Robustheitsprüfungen** (Art. 10, Art. 15).
10. **Keine Dokumentation zur Konformitätsbewertung/Registrierung** (Art. 43, 48, 49).

---

13. Maßnahmen und Handlungsempfehlungen

Bereits geltend (höchste Priorität, sofort umzusetzen)

1. **Sofortige Einführung menschlicher Überprüfung** vor jeder automatischen Ablehnung - Beendigung der vollautomatisierten Entscheidung (Art. 22 DSGVO, gilt bereits).
2. **Klärung der Fotoverarbeitung** - Prüfung, ob Emotionserkennung/biometrische Kategorisierung vorliegt; im Zweifel sofortige Aussetzung dieser Funktion (Art. 5 AI Act, gilt seit 02.02.2025).
3. **Nachholung der KI-Kompetenz-Schulungen** für Recruiter und Verantwortliche (Art. 4 AI Act, gilt seit 02.02.2025).
4. **Durchführung einer DSFA** nach Art. 35 DSGVO (gilt bereits).
5. **Information des Betriebsrats** über den Systemeinsatz (BetrVG/Art. 26 Abs. 7, mitbestimmungsrelevant, unabhängig von AI-Act-Stichtag umzusetzen).

Gilt ab 02.08.2026 (unmittelbar bevorstehend - vor Stichtag abzuschließen)

6. **Klärung und Dokumentation der Doppelrolle** (Anbieter gem. Art. 25 Abs. 1 lit. c + Betreiber) und Ableitung aller Anbieterpflichten.
7. **Aufbau eines Risikomanagementsystems** (Art. 9).
8. **Daten-Governance-Prüfung inkl. Bias-Analyse** der Trainingsdaten (Art. 10).
9. **Erstellung von Betriebsanleitung, technischer Dokumentation und Logging-Konzept** (Art. 11-13).
10. **Konformitätsbewertung, CE-Kennzeichnung, Registrierung in EU-Datenbank** (Art. 43, 48, 49).
11. **Vertragliche Klärung mit US-Basismodell-Anbieter** gemäß Art. 25 Abs. 4.
12. **Klärung internationaler Datenflüsse** (Kapitel V DSGVO).

Offene Punkte/nachzufordernde Nachweise

- Zweckbestimmung und technische Funktionsweise der Fotoverarbeitung.
- Vertragsunterlagen mit dem US-LLM-Anbieter.
- Nachweise zu Trainingsdaten-Herkunft und Bias-Tests.
- Bestätigung, ob Auftraggeber/Betreiber ein Finanzunternehmen ist (DORA-Prüfung).
- Klärung, ob eine FRIA-Pflicht mangels öffentlichen Dienstbezugs tatsächlich entfällt (bestätigt: entfällt) und DSFA als Ersatzinstrument dokumentiert wird.

Diese Analyse ist ein fachliches Hilfsergebnis und ersetzt keine Rechtsberatung.

Prüfgrundlage

Modell: anthropic/claude-sonnet-5 - 0.2.0 - 2026-07-05T09:43:47
- systembeschreibung.txt (1 Blöcke, SHA-256 ade2e773bea0...)

Rechtsstand des Normtext-Korpus

- DSGVO: CELEX 02016R0679-20160504 (abgerufen 2026-07-04)
- EU AI Act: CELEX 32024R1689 (abgerufen 2026-07-04)
- DORA: CELEX 32022R2554 (abgerufen 2026-07-04)

Diese Analyse ist ein fachliches Hilfsergebnis und ersetzt keine Rechtsberatung. Hochrisiko-Einstufungen ersetzen nicht das Konformitätsbewertungsverfahren nach Art. 43 AI Act. Alle Befunde sind vor Weitergabe fachlich zu prüfen.