

Arbeitsakte

Akte: KI-Governance Konzern-Rollout — Thalheim Industries SE

ki-governance-konzern-rollout-thalheim-industries

Die ZIP-URL ist stabil und zeigt immer auf die aktuelle Version. Im Akten-ZIP ist das Gesamt-PDF mit enthalten.

Diese Datei bündelt alle Aktenstücke in einem Dokument. Die Einzeldateien liegen im Aktenordner ebenfalls vor.

Inhaltsverzeichnis

Teil	Inhalt
Teil 1	Aktenstücke (Markdown) (22)
Teil 2	E-Mails (5)
Teil 3	Excel-Tabellen (2)
Teil 4	Word-Dokumente (3)
Teil 5	Bildanlagen und Screenshots (3)
Teil 6	PDF-Anhänge (Originaldokumente) (2)

Aktenstücke (Markdown)

Datei: 01-governance-leitlinie-entwurf.md

KI-Governance-Leitlinie Thalheim Industries SE — Entwurf v2.1

Aktenzeichen: TI-KI-2026-007

Dokumentversion: 2.1 (Entwurf, freigegeben zur Konsultation)

Erstellungsdatum: 10. Februar 2026

Verfasser: Dr. Falk Roosendaal, KI-Komitee-Vorsitz; Annegret Kühnhausen, CCO

Freigabe ausstehend: Vorstand (geplant 15. April 2026)

1. Zweck und Geltungsbereich

Diese Leitlinie regelt den verantwortungsvollen Einsatz von Systemen künstlicher Intelligenz (KI-Systeme) innerhalb der Thalheim Industries SE sowie aller in- und ausländischen Tochtergesellschaften, sofern diese in der EU tätig sind oder EU-Bürger als Nutzer oder Betroffene haben.

Die Leitlinie dient der Umsetzung der Anforderungen der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über künstliche Intelligenz (KI-Verordnung, KI-VO) sowie der ergänzenden datenschutzrechtlichen Anforderungen aus der Datenschutz-Grundverordnung (DSGVO, Verordnung (EU) 2016/679).

Sie schafft konzernweit verbindliche Mindeststandards für:

- die Inventarisierung und Klassifikation von KI-Systemen (vgl. Abschnitt 3);
- die Risikosteuerung, insbesondere bei Hochrisiko-KI-Systemen nach Art. 6 i.V.m. Anhang III KI-VO;
- die Erfüllung von Betreiber- und Anbieterpflichten nach Art. 9–17 KI-VO;
- die Sicherstellung von KI-Kompetenz bei allen Mitarbeiterinnen und Mitarbeitern nach Art. 4 KI-VO;
- die Integration in bestehende Compliance- und Datenschutzprozesse.

Diese Leitlinie gilt für alle Beschäftigten, Führungskräfte, Auftragnehmer und Dienstleister, die KI-Systeme im Auftrag oder für Zwecke der Thalheim Industries SE einsetzen.

2. Grundsätze

Der Einsatz von KI-Systemen bei Thalheim Industries SE richtet sich nach folgenden Grundsätzen:

2.1 Rechtmäßigkeit: KI-Systeme werden nur eingesetzt, wenn sie die anwendbaren Rechtsvorschriften einhalten, insbesondere die KI-VO, die DSGVO sowie sektorspezifische Regulierung (z. B. Kreditwesengesetz, Finanzmarktregulierung).

2.2 Menschliche Aufsicht: Bei allen Hochrisiko-KI-Systemen nach Art. 6 i.V.m. Anhang III KI-VO ist eine wirksame menschliche Aufsicht nach Art. 14 KI-VO sicherzustellen. KI-Systeme treffen keine

abschließenden Entscheidungen mit wesentlichen Folgen für natürliche Personen ohne Möglichkeit menschlicher Überprüfung und Korrektur.

2.3 Transparenz: Der Einsatz von KI-Systemen, insbesondere gegenüber betroffenen Personen, ist in angemessener Weise offenzulegen. Für KI-Systeme mit Transparenzpflichten nach Art. 50 KI-VO (Chatbots, synthetische Inhalte) sind entsprechende Hinweispflichten umzusetzen.

2.4 Nicht-Diskriminierung und Fairness: KI-Systeme, die in personenbezogenen Entscheidungsprozessen eingesetzt werden (insbesondere RecruitAI), sind auf Verzerrungen (Bias) zu testen und zu überwachen. Systematische Diskriminierungen nach Art. 9 Abs. 7 KI-VO sind zu vermeiden.

2.5 Datenschutz by Design: Die Einführung neuer KI-Systeme erfolgt unter Einbeziehung der Datenschutzbeauftragten Dr. Carla Eichenmüller ab der Planungsphase. Soweit erforderlich, ist eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen.

2.6 Nachhaltigkeit und Rechenschaftspflicht: Der Vorstand trägt die Gesamtverantwortung für die KI-Governance im Konzern. Die Geschäftsleitung haftet nach § 93 Abs. 1 AktG für die Einhaltung dieser Leitlinie (vgl. Literaturverweis: <https://dejure.org/gesetze/AktG/93.html>).

3. KI-Inventar und Klassifikation

3.1 KI-Inventar: Sämtliche im Konzern eingesetzten KI-Systeme sind im zentralen KI-Inventar zu registrieren und zu pflegen. Das CDO-Büro (Marcus Petersen) verantwortet die technische Führung des Inventars. Die Erstinventarisierung wurde im Rahmen der Projektphase 1 (Oktober–Dezember 2025) durchgeführt; 23 Systeme wurden erfasst.

3.2 Risikoklassifikation: Jedes KI-System ist nach dem Risikoschema der KI-VO einzustufen:

Risikoklasse	Grundlage KI-VO	Beispiel Thalheim
Unannehmbares Risiko (verboten)	Art. 5 KI-VO	— (keines identifiziert)
Hochrisiko	Art. 6, Anh. III KI-VO	RecruitAI, CreditVision Score
Begrenztes Risiko	Art. 50 KI-VO	ServiceBot, CodeAssist, PredictMaint
Minimales Risiko	—	Spam-Filter, Rechtschreibkorrektur

Die vollständige Klassifikationsmatrix ist in Aktenstück 02 (TI-KI-2026-008) dokumentiert.

3.3 Neueinführungen: Jede Neueinführung oder wesentliche Änderung eines KI-Systems erfordert einen KI-Freigabeprozess (KI-Clearance), der eine Risikoklassifikation, eine datenschutzrechtliche Vorabprüfung und — bei Hochrisiko — eine vollständige Konformitätsprüfung umfasst.

4. Governance-Struktur

4.1 KI-Komitee: Das KI-Komitee (Vorsitz: Dr. Falk Roosendaal) ist das zentrale Steuerungsgremium für alle Fragen der KI-Governance. Es tagt quartalsweise und bei Bedarf. Mitglieder sind: CIO Dr. Wolfsbacher, CDO Marcus Petersen, CCO Annegret Kühnhausen, DSB Dr. Eichenmüller sowie Vertreter der Fachbereiche.

4.2 Verantwortlichkeiten:

Rolle	Funktion	Zuständigkeit
CEO Dr. Thalheim-Lattermann	Vorstand	Gesamtverantwortung, AktG § 93
CIO Dr. Wolfsbacher	Technik	KI-Infrastruktur, Auditbereitschaft
CDO Marcus Petersen	Daten	KI-Inventar, Datenqualität
CCO Annegret Kühnhausen	Compliance	KI-VO-Konformität, Behördenkontakt
DSB Dr. Eichenmüller	Datenschutz	DSGVO, DPIA, LfDI-Kontakt
KI-Komitee-Vorsitz Dr. Roosendaal	Governance	Koordination, Eskalation
Betriebsrat (Norbert Schäpers)	Mitbestimmung	§ 87 BetrVG, Betriebsvereinbarung

4.3 Betriebsrat: Der Betriebsrat ist gemäß § 87 Abs. 1 Nr. 6 BetrVG

(<https://dejure.org/gesetze/BetrVG/87.html>) bei der Einführung und wesentlichen Änderung technischer Einrichtungen, die zur Überwachung des Verhaltens oder der Leistung der Arbeitnehmer bestimmt sind oder geeignet sind, frühzeitig einzubeziehen. Dies gilt ausdrücklich für RecruitAI und CreditVision Score.

5. Verbotene Praktiken

In Übereinstimmung mit Art. 5 KI-VO (<https://dejure.org/gesetze/KIVO/5.html>) sind bei Thalheim Industries SE folgende KI-Praktiken verboten:

- KI-Systeme zur unterschweligen Beeinflussung von Personen ohne deren Wissen;
- Systeme zur Ausnutzung von Vulnerabilitäten von Personen;
- Social Scoring-Systeme durch Behörden oder vergleichbare private Einstufungen;
- Echtzeit-Fernererkennung biometrischer Merkmale in öffentlich zugänglichen Räumen;
- Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen.

Eine vollständige Rote Liste mit Prüfschema findet sich in Aktenstück 09 (TI-KI-2026-013).

6. Pflichten für Hochrisiko-KI-Systeme

Für alle Hochrisiko-KI-Systeme (derzeit: RecruitAI, CreditVision Score) gelten kumulativ die Anforderungen nach Art. 9–17 KI-VO:

- **Art. 9:** Risikomanagementsystem — laufend, dokumentiert;
- **Art. 10:** Daten-Governance — Trainings- und Testdaten dokumentiert, repräsentativ;
- **Art. 11:** Technische Dokumentation — vollständig, aktuell (Vorlage 72 h nach Anforderung durch Behörden);
- **Art. 12:** Aufzeichnungs- und Protokollierungspflichten — automatische Protokollierung aktiviert;
- **Art. 13:** Transparenz gegenüber Betreibern — Gebrauchsanweisung vorhanden;
- **Art. 14:** Menschliche Aufsicht — technisch und organisatorisch implementiert;
- **Art. 15:** Genauigkeit, Robustheit, Cybersicherheit — regelmäßige Tests, Penetrationstests;

- **Art. 16:** Betreiberpflichten — Registrierung, Konformitätsbewertung vor Inbetriebnahme;
- **Art. 17:** Qualitätsmanagementsystem — ISO-konformes QMS vorhanden.

Die Konformitätsbewertung nach Art. 43 Abs. 2 KI-VO (interne Bewertung für HR-/Kreditssysteme) wird durch die WPG Hagedorn & Partner als externen Auditor begleitet.

7. AI Literacy (Art. 4 KI-VO)

Alle Mitarbeiterinnen und Mitarbeiter, die KI-Systeme einsetzen oder beaufsichtigen, müssen über ausreichende KI-Kompetenz verfügen (Art. 4 KI-VO, <https://dejure.org/gesetze/KIVO/4.html>). Das Curriculum ist in Aktenstück 05 (TI-KI-2026-009) beschrieben. Die Schulungspflicht ist bis 31.10.2026 flächendeckend zu erfüllen.

8. Schatten-KI und nicht genehmigte Systeme

Mitarbeiterinnen und Mitarbeiter dürfen keine KI-Systeme einsetzen, die nicht im KI-Inventar registriert und durch den KI-Freigabeprozess freigegeben wurden. Verstöße sind unverzüglich der CCO Kühnhausen zu melden und können arbeitsrechtliche Konsequenzen haben. Der Vorfall in der Marketingabteilung (März 2026, Aktenstück 16) zeigt die praktische Relevanz dieser Regelung.

9. Inkrafttreten und Überprüfung

Diese Leitlinie tritt nach Freigabe durch den Vorstand (geplant 15. April 2026) in Kraft. Sie wird jährlich überprüft und bei wesentlichen Änderungen der Rechtslage oder des KI-Einsatzes anlassbezogen angepasst.

Nächste planmäßige Überprüfung: April 2027.

Erstellt im Rahmen des Compliance-Programms TI-KI-2026, Thalheim Industries SE. Aktenzeichen: TI-KI-2026-007. Externe Rechtsberatung: Kanzlei Borchmann Compliance, Frankfurt am Main.

Datei: 02-risikoklassifikations-matrix.md

Risikoklassifikationsmatrix KI-Systeme — Thalheim Industries SE

Aktenzeichen: TI-KI-2026-008

Dokumentversion: 1.4

Erstellungsdatum: 18. Dezember 2025

Verfasser: Dr. Falk Roosendaal; Marcus Petersen (CDO); Annegret Kühnhausen (CCO)

Freigegeben durch: KI-Komitee, 10. Januar 2026

1. Zweck

Dieses Dokument enthält die vollständige Risikoklassifikation aller im KI-Inventar der Thalheim Industries SE erfassten KI-Systeme gemäß der Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-VO). Die Klassifikation folgt dem vierstufigen Risikoschema der KI-VO (Art. 5, Art. 6 i.V.m. Anhang III, Art. 50, Minimales Risiko).

Rechtsgrundlagen:

- Art. 6 i.V.m. Anhang III KI-VO (Hochrisiko-Klassifikation): <https://dejure.org/gesetze/KIVO/6.html>
- Art. 5 KI-VO (Verbotene Praktiken): <https://dejure.org/gesetze/KIVO/5.html>
- Art. 50 KI-VO (Transparenzpflichten): <https://dejure.org/gesetze/KIVO/50.html>

2. Klassifikationsschema

Die Einordnung erfolgt nach einem dreistufigen Prüfschema:

Stufe 1 — Verboten (Art. 5 KI-VO): Fällt das System unter eine der verbotenen Praktiken? → Sofortiger Stopp, keine weitere Prüfung.

Stufe 2 — Hochrisiko (Art. 6 i.V.m. Anh. III KI-VO):

- Ist das System ein Sicherheitsbauteil eines Produkts nach Anhang I? → Hochrisiko.
- Fällt es unter eine der acht Kategorien des Anhangs III? → Hochrisiko, sofern es bei natürlichen Personen individuelle Entscheidungen beeinflusst oder eigenständig trifft.

Stufe 3 — Transparenzpflichten (Art. 50 KI-VO):

- Chatbots / Konversationssysteme → Offenlegungspflicht.
- Deep-Fake-Generatoren / synthetische Inhalte → Kennzeichnungspflicht.

Alle nicht in Stufe 1–3 fallenden Systeme gelten als Systeme mit minimalem Risiko.

3. Klassifikationsergebnisse: Fünf Kernsysteme

3.1 RecruitAI (Recruiting-Screening)

Merkmal	Inhalt
Vendor	Synaptec Analytics GmbH, München
Einsatzbereich	HR / Personalauswahl
Funktion	Automatisiertes Screening von Bewerbungsunterlagen, Ranking-Score
Prüfung Art. 5	Keine verbotene Praktik (kein Social Scoring, keine unterschwellige Beeinflussung)
Prüfung Art. 6 / Anh. III	Anh. III Nr. 4a: „KI-Systeme zur Personalauswahl, zur Priorisierung von Kandidaten“ → **Hochrisiko**
Einstufung	**Hochrisiko**
Rechtsgrundlage	Art. 6 Abs. 2, Anhang III Nr. 4 lit. a KI-VO
Konformitätsfrist	02. August 2026
Konformitätsbewertung	Intern nach Art. 43 Abs. 2 KI-VO; Auditor: Hagedorn & Partner
DPIA erforderlich	Ja — Art. 35 DSGVO; Aufforderung LfDI BW AZ 1-1085.51/2026/045

Merkmal	Inhalt
Verantwortlicher	Dr. Sigrid Wolfsbacher (CIO)
Status (März 2026)	Audit läuft; Feststellung fehlender Bias-Tests

Begründung: RecruitAI trifft oder beeinflusst maßgeblich Entscheidungen über die Aufnahme oder Ablehnung von Bewerbern. Anhang III Nr. 4 lit. a KI-VO erfasst explizit KI-gestützte Systeme zur „Zulassung zu Beschäftigung“ und zur „Priorisierung von Bewerbern“. Die Hochrisiko-Einstufung ist eindeutig. Eine DPIA ist nach Art. 35 Abs. 3 lit. a DSGVO (systematische Bewertung persönlicher Aspekte) erforderlich. Art. 22 DSGVO (automatisierte Einzelentscheidungen) ist im Lichte von Art. 26 KI-VO zu lesen.

3.2 CreditVision Score (Kreditscoring-Modul)

Merkmal	Inhalt
Vendor	CreditVision AG, Frankfurt am Main
Einsatzbereich	Kundenfinanzierung / Kreditentscheidung
Funktion	Scoring-Modell zur Bonitätsbewertung von Privat- und Gewerbekunden
Prüfung Art. 5	Keine verbotene Praktik
Prüfung Art. 6 / Anh. III	Anh. III Nr. 5b: „KI-Systeme zur Bewertung der Kreditwürdigkeit natürlicher Personen“ → Hochrisiko
Einstufung	Hochrisiko
Rechtsgrundlage	Art. 6 Abs. 2, Anhang III Nr. 5 lit. b KI-VO
Konformitätsfrist	02. August 2026
Konformitätsbewertung	Intern nach Art. 43 Abs. 2 KI-VO; Auditor: Hagedorn & Partner
DPIA erforderlich	Prüfung läuft (hohe Wahrscheinlichkeit)
Verantwortlicher	Marcus Petersen (CDO)
Status (März 2026)	Offene BaFin-Anfrage GZ BJ 24-K 7102-2026/0012; Unterlagen CreditVision AG ausstehend

Begründung: Das Kreditscoring-Modul wird zur Bewertung der Kreditwürdigkeit natürlicher Personen eingesetzt und beeinflusst damit Entscheidungen mit erheblichen Rechts- oder vergleichbar erheblichen Folgen für die Betroffenen. Art. 22 DSGVO (<https://dejure.org/gesetze/DSGVO/22.html>) und Art. 6 i.V.m. Anh. III Nr. 5b KI-VO gelten kumulativ. Die BaFin prüft im Rahmen ihrer Aufsicht (GZ BJ 24-K 7102-2026/0012) die Einhaltung von Art. 22 DSGVO und die Konformitätsbewertung nach Art. 43 KI-VO.

3.3 PredictMaint (Predictive Maintenance)

Merkmal	Inhalt
Vendor	Intern entwickelt (Thalheim Digital Lab)
Einsatzbereich	Produktionsanlagen / Wartungsplanung
Funktion	Anomalieerkennung, Verschleißprognose auf Basis von Sensordaten
Prüfung Art. 5	Keine verbotene Praktik

Merkmal	Inhalt
Prüfung Art. 6 / Anh. III	Kein Anhang-III-Tatbestand; kein Sicherheitsbauteil i.S.v. Anhang I
Einstufung	**Begrenztes Risiko**
Transparenzpflichten	Keine nach Art. 50 KI-VO (kein Chatbot, keine synthetischen Inhalte)
Anmerkung	Hohe wirtschaftliche Relevanz, aber kein personenbezogener Entscheidungseinfluss
Verantwortlicher	Dr. Sigrid Wolfsbacher (CIO)
Konformitätsfrist	02. August 2027 (freiwillige interne Überprüfung)

Begründung: PredictMaint verarbeitet ausschließlich Maschinendaten und trifft keine Entscheidungen über natürliche Personen. Ein Anhang-III-Tatbestand liegt nicht vor. Das System fällt damit nicht unter die Hochrisiko-Kategorie. Empfehlung: Freiwillige Dokumentation im Rahmen des KI-Inventars und Überprüfung bis August 2027.

3.4 CodeAssist (GenAI-Coding-Assistent)

Merkmal	Inhalt
Vendor	OpenAI Ireland Ltd., Dublin (GPT-4-basiert)
Einsatzbereich	Software-Entwicklung intern
Funktion	KI-gestützte Code-Generierung und Code-Review
Prüfung Art. 5	Keine verbotene Praktik
Prüfung Art. 6 / Anh. III	Kein Anhang-III-Tatbestand
Einstufung	**Begrenztes Risiko** (Allzweck-KI-Modell nach Art. 51 ff. KI-VO)
Transparenzpflichten	Art. 50 Abs. 2 KI-VO: Kennzeichnung KI-generierter Inhalte (Code-Kommentare)
Vendor-Pflichten	OpenAI als Anbieter unterliegt Art. 53 ff. KI-VO (GPAI-Modell-Pflichten)
Verantwortlicher	Marcus Petersen (CDO)
Status (März 2026)	Konformitätsdokumentation OpenAI unvollständig; Nachforderung läuft

Begründung: CodeAssist basiert auf einem Allzweck-KI-Modell (GPAI) im Sinne von Art. 3 Nr. 63 KI-VO. Als Betreiber (Deployer) ist Thalheim nach Art. 26 KI-VO verantwortlich für die zweckgerechte Nutzung. OpenAI unterliegt als Anbieter (Provider) des Basismodells den Pflichten nach Art. 53 KI-VO. Thalheim muss sicherstellen, dass die Nutzung den Nutzungsbedingungen von OpenAI entspricht und keine personenbezogenen Daten ohne Rechtsgrundlage verarbeitet werden.

3.5 ServiceBot (Kundenservice-Chatbot)

Merkmal	Inhalt
Vendor	Intern entwickelt (Thalheim Digital Lab)
Einsatzbereich	Kundenservice / First-Level-Support
Funktion	Automatisierte Beantwortung von Kundenanfragen
Prüfung Art. 5	Keine verbotene Praktik

Merkmal	Inhalt
Prüfung Art. 6 / Anh. III	Kein Anhang-III-Tatbestand (kein Entscheidungseinfluss auf Betroffene)
Einstufung	**Transparenzpflichten (Art. 50 KI-VO)**
Transparenzpflichten	Art. 50 Abs. 1 KI-VO: Kunden müssen informiert werden, dass sie mit einem KI-System interagieren
Umsetzungsstand	Hinweis implementiert seit 01.02.2025; Dokumentation in TI-KI-2026-007
Verantwortlicher	Marcus Petersen (CDO)

Begründung: ServiceBot ist ein konversationelles KI-System im Sinne von Art. 50 Abs. 1 KI-VO. Die Pflicht zur Offenlegung gegenüber natürlichen Personen gilt unabhängig von der Risikoklasse. Die Umsetzung erfolgte fristgerecht (Art. 113 Abs. 3 KI-VO: Anwendung von Art. 50 ab 02.02.2025). Eine vollständige Überprüfung der Umsetzung findet im Rahmen des Q2-2026-Audits statt.

4. Weitere klassifizierte Systeme (Auszug)

Zusätzlich zu den fünf Kernsystemen wurden im Rahmen der Inventarisierung (Phase 1) folgende Systeme klassifiziert:

System	Einsatzbereich	Risikoklasse	Bemerkung
MarketingAI (Midjourney-basiert)	Marketing	Begrenztes Risiko / **ungenehmigt**	Schatten-KI; identifiziert März 2026
AutoTranslate	Übersetzung intern	Minimales Risiko	Keine DPIA, keine Freigabepflicht
FinanceReport-AI	Controlling	Minimales Risiko	Keine Entscheidungsau- tomation
EnergyForecast	Energiemanagement	Minimales Risiko	Keine Personenbezogenheit
QualityVision	Qualitätskontrolle	Begrenztes Risiko	Optisches System, keine Personenerkennung

5. Anwendungsfristen (Art. 113 KI-VO)

Datum	Regelung
02.02.2025	Art. 5 (Verbote), Art. 50 (Transparenz) anwendbar
02.08.2025	Governance-Pflichten (Kapitel I, II), Art. 4 (AI Literacy) anwendbar
02.08.2026	Hochrisiko-Pflichten (Art. 6, 9–17, 43) anwendbar für neue Systeme; bestehende Hochrisiko-Systeme müssen nachkonformiert sein
02.08.2027	Hochrisiko-Systeme nach Anhang I (bestehende Produkte)

Quelle: Art. 113 KI-VO (<https://dejure.org/gesetze/KIVO/113.html>).

Datei: 03-vorstandsbeschluss.md

Vorstandsbeschluss — KI-Governance-Programm TI-KI-2026

Aktenzeichen: TI-KI-2026-007 (Unterlage zum Vorstandsbeschluss)

Datum: 15. Oktober 2025

Gremium: Vorstand der Thalheim Industries SE

Beschlusnummer: VS-2025-087

Protokollführerin: Claudia Berger-Hentschel, Vorstandsassistentin

Anwesende Vorstandsmitglieder

- Dr. Reinhard Thalheim-Lattermann (Vorsitzender, CEO)
- Dr. Sigrid Wolfsbacher (CIO)
- Marcus Petersen (CDO)
- Annegret Kühnhausen (CCO / Chief Compliance Officer)
- Klaus-Dieter Obermaier (CFO)
- Prof. Dr. Karin Schirrmeister (COO)

Gegenstand des Beschlusses

Der Vorstand fasst sich mit der Umsetzung der Anforderungen aus der Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-VO) für die Thalheim Industries SE und alle Konzerngesellschaften. Die KI-VO enthält gestaffelte Anwendungsfristen (Art. 113 KI-VO); insbesondere treten die Pflichten für Hochrisiko-KI-Systeme am 02. August 2026 in Kraft. Der Vorstand sieht erheblichen Handlungsbedarf.

Beschlossene Maßnahmen

Der Vorstand beschließt einstimmig:

1. Einrichtung KI-Governance-Programm TI-KI-2026

Es wird ein konzernweites KI-Governance-Programm unter dem Kürzel **TI-KI-2026** eingerichtet. Programmlaufzeit: Oktober 2025 bis Dezember 2027. Das Programm gliedert sich in drei Phasen:

- **Phase 1** (Oktober–Dezember 2025): Inventarisierung aller KI-Systeme, Risikoklassifikation, Gap-Analyse.
- **Phase 2** (Januar–Dezember 2026): Konformitätsherstellung für Hochrisiko-Systeme, DPIA, Betriebsvereinbarung, AI-Literacy-Schulung.
- **Phase 3** (Januar–Dezember 2027): Konsolidierung, Audit-Readiness, Governance-Optimierung.

2. Ernennung KI-Komitee-Vorsitz

Dr. Falk Roosendaal (Leiter Governance & Risk) wird zum Vorsitzenden des neu einzurichtenden KI-Komitees ernannt. Das KI-Komitee tagt quartalsweise und berichtet an den Vorstand. Erste Sitzung: 15. Januar 2026.

3. Externe Rechtsberatung

Kanzlei Borchmann Compliance (Frankfurt) wird mandatiert, die KI-VO-Implementierung zu begleiten und Stellungnahmen gegenüber Behörden (BaFin, LfDI BW) zu koordinieren. Budget: bis zu 280.000 EUR für die Programmlaufzeit.

4. Externe Prüfung / Auditor

Die Wirtschaftsprüfungsgesellschaft Hagedorn & Partner wird mandatiert, die Konformitätsbewertung für RecruitAI und CreditVision Score nach Art. 43 Abs. 2 KI-VO zu begleiten. Erster Prüfbericht bis 31. März 2026.

5. Budget

Das Programm-Gesamtbudget für Phase 1 und 2 beträgt 1.450.000 EUR (inkl. Personalaufwand intern, externe Beratung, Technologie-Anpassungen, Schulungen). Detaillierter Budgetplan in Aktenstück 21.

6. Erklärung zur Vorstandshaftung

Der Vorstand ist sich bewusst, dass eine Verletzung der Betreiberpflichten nach der KI-VO zu Bußgeldern von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes führen kann (Art. 99 KI-VO). Die Vorstandsmitglieder sind nach § 93 Abs. 1 AktG (<https://dejure.org/gesetze/AktG/93.html>) verpflichtet, die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Der Vorstand erklärt, das Programm TI-KI-2026 als prioritär einzustufen.

7. Berichterstattung an Aufsichtsrat

Der CCO erstattet dem Aufsichtsrat quartalsweise Bericht über den Programmfortschritt. Erster Aufsichtsratsbericht: Q1 2026 (März 2026), dokumentiert in Aktenstück 12.

8. Betriebsrat

Der Vorstand beauftragt die CCO, unverzüglich Verhandlungen mit dem Betriebsrat über eine Betriebsvereinbarung KI aufzunehmen, um die Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 6 BetrVG (<https://dejure.org/gesetze/BetrVG/87.html>) zu wahren und einen geordneten Rollout der Hochrisiko-Systeme zu ermöglichen.

Votum

Vorstandsmitglied	Position	Votum
Dr. Thalheim-Lattermann	CEO	Ja
Dr. Wolfsbacher	CIO	Ja
Marcus Petersen	CDO	Ja
Annegret Kühnhausen	CCO	Ja
Klaus-Dieter Obermaier	CFO	Ja (mit Vorbehalt Budgetprüfung Q1 2026)
Prof. Dr. Schirrmeister	COO	Ja

Beschluss einstimmig angenommen. CFO-Vorbehalt zu Protokoll.

Anlagen zum Beschluss

1. Präsentation CIO/CCO: „KI-VO — Handlungsbedarf Thalheim Industries SE" (18 Folien, intern)
2. Übersicht KI-Systeme Thalheim (Vorab-Inventar, Stand Oktober 2025, 7 Seiten)
3. Angebot Kanzlei Borchmann Compliance (vertraulich)
4. Angebot Hagedorn & Partner (vertraulich)

*Beschluss-Nr. VS-2025-087. Protokoll genehmigt vom Vorstand am 29. Oktober 2025.
Aufbewahrungs-AZ: TI-KI-2026-007.*

Datei: 04-pflichtenmatrix-fachbereiche.md

Pflichtenmatrix — Betreiberpflichten nach Art. 9 ff. KI-VO je Fachbereich

Aktenzeichen: TI-KI-2026-009

Dokumentversion: 1.2

Erstellungsdatum: 20. Januar 2026

Verfasser: Annegret Kühnhausen (CCO); Dr. Falk Roosendaal

Stand: März 2026

1. Einleitung

Diese Pflichtenmatrix weist die Betreiberpflichten (Deployer-Pflichten) nach Art. 9 ff. KI-VO sowie Art. 26 KI-VO für die Hochrisiko-KI-Systeme der Thalheim Industries SE den verantwortlichen Fachbereichen zu. Die Matrix dient als Arbeitsgrundlage für die Konformitätsherstellung bis 02.08.2026.

Rechtsgrundlagen (Auszug):

- Art. 9 KI-VO — Risikomanagementsystem: <https://dejure.org/gesetze/KIVO/9.html>
- Art. 26 KI-VO — Pflichten von Betreibern: <https://dejure.org/gesetze/KIVO/26.html>
- Art. 35 DSGVO — Datenschutz-Folgenabschätzung: <https://dejure.org/gesetze/DSGVO/35.html>

Fokus: RecruitAI (Hochrisiko, Anh. III Nr. 4a) und CreditVision Score (Hochrisiko, Anh. III Nr. 5b). Für PredictMaint, CodeAssist und ServiceBot gelten vereinfachte Anforderungen (vgl. Abschnitt 5).

2. Pflichtenkatalog Hochrisiko-Systeme

2.1 Pflichtensteckbrief RecruitAI

System: RecruitAI — Recruiting-Screening-Tool

Vendor: Synaptec Analytics GmbH

Betreiber (Deployer): Thalheim Industries SE, Fachbereich HR

Interne Systemverantwortliche: Barbara Trenkmann (Leiterin HR-Systeme)

Art. KI-VO	Pflicht	Verantwortlich	Frist	Status (März 2026)
Art. 9	Risikomanagementsystem dokumentieren und aufrechterhalten	HR / Compliance	02.06.2026	In Bearbeitung
Art. 9 Abs. 7	Bias-Tests durchführen (Diskriminierung, Fairness)	HR / IT / Audit	02.06.2026	**Offen — Mangel festgestellt**
Art. 10	Daten-Governance prüfen (Trainings- u. Testdaten)	CDO / HR	30.04.2026	Teilweise erledigt
Art. 11	Technische Dokumentation vollständig? (Vendor-Dokument)	CIO / Vendor	30.04.2026	Synaptec-Unterlagen angefordert
Art. 12	Protokollierungspflicht aktiviert	IT / CIO	31.03.2026	Umgesetzt
Art. 13	Gebrauchsanweisung vorhanden und verständlich?	HR	30.04.2026	Vorhanden (DE-Version Synaptec)
Art. 14	Menschliche Aufsicht implementiert (technisch + organisatorisch)	HR / IT	30.06.2026	Konzept in Erarbeitung
Art. 14 Abs. 4	HR-Entscheider kann System abschalten / überstimmen	HR	30.06.2026	Technisch möglich, SOP fehlt
Art. 15	Genauigkeit, Robustheit und Cybersicherheit testen	IT-Security / CIO	30.06.2026	Pentest ausstehend
Art. 26 Abs. 4	Betreiber informiert Behörden bei Vorfällen (Art. 73 KI-VO)	CCO	Laufend	Prozess definiert

Art. KI-VO	Pflicht	Verantwortlich	Frist	Status (März 2026)
Art. 26 Abs. 7	Betreiber meldet Konformitätsmängel an Marktüberwachung	CCO	Laufend	Keine Meldepflicht aktuell
Art. 35 DSGVO	DPIA durchgeführt und vorliegend	DSB Dr. Eichenmüller	30.06.2026	In Erarbeitung
Art. 22 DSGVO	Automatisierte Entscheidung: Recht auf Erklärung umgesetzt	HR / DSB	30.06.2026	Kandidatenmitteilung angepasst
§ 87 BetrVG	Mitbestimmung: Betriebsvereinbarung abgeschlossen?	CCO / Betriebsrat	Vor Rollout	**Offen — BR blockiert**

2.2 Pflichtensteckbrief CreditVision Score

System: CreditVision Score — Kreditscoring-Modul

Vendor: CreditVision AG

Betreiber (Deployer): Thalheim Industries SE, Fachbereich Finanzierung / Vertrieb

Interne Systemverantwortliche: Rolf Haselmann (Leiter Kundenfinanzierung)

Art. KI-VO	Pflicht	Verantwortlich	Frist	Status (März 2026)
Art. 9	Risikomanagementsystem	Finanzierung / Compliance	02.06.2026	Entwurf CreditVision erhalten
Art. 9 Abs. 7	Bias-Tests Kreditvergabe	Finanzierung / CDO	02.06.2026	CreditVision-Auskunft ausstehend
Art. 10	Daten-Governance: Kunden-Trainingsdaten geprüft?	CDO	30.04.2026	Nein — in Prüfung
Art. 11	Technische Dokumentation (Vendor)	Finanzierung / CIO	30.04.2026	Unterlagen CreditVision unvollständig
Art. 12	Protokollierung aktiviert	IT	31.03.2026	Umgesetzt
Art. 13	Gebrauchsanweisung	Finanzierung	30.04.2026	Vorhanden

Art. KI-VO	Pflicht	Verantwortlich	Frist	Status (März 2026)
Art. 14	Menschliche Aufsicht: Kreditscheider hat Letztentscheid	Finanzierung	30.06.2026	Ja, prozessual verankert
Art. 22 DSGVO	Automatisierte Einzelentscheidung: Widerspruchsr echt informiert	Finanzierung / DSB	Sofort	Datenschutzhinweis aktualisiert
Art. 43 Abs. 2	Interne Konformitätsbewertung (durch Auditor begleitet)	CCO / Hagedorn	31.07.2026	Audit geplant Mai 2026
BaFin GZ BJ 24-K	Stellungnahme an BaFin	CCO / Borchmann	15.05.2026	In Vorbereitung
§ 87 BetrVG	Mitbestimmung	CCO / Betriebsrat	Vor Rollout	**Offen — BR blockiert**

3. Fachbereichsverantwortlichkeiten

Fachbereich	KI-System(e)	Ansprechpartner	Kernpflicht bis 02.08.2026
HR / Personal	RecruitAI	Barbara Trenkmann	Art. 14 Aufsicht; Art. 9 Bias-Tests
Kundenfinanzierung	CreditVision Score	Rolf Haselmann	Art. 14 Aufsicht; Art. 22 DSGVO
IT / Digital	PredictMaint, CodeAssist, ServiceBot	Marcus Petersen (CDO)	Transparenzpflichten Art. 50
Compliance	Alle	Annegret Kühnhausen	Koordination, Behördenkontakt
Datenschutz	RecruitAI (DPIA)	Dr. Carla Eichenmüller	Art. 35 DSGVO bis 30.06.2026
Revision	Alle	Franz-Josef Brammer	Interne Kontrolle, Schatten-KI

4. Eskalationsmatrix

Risiko	Auslöser	Eskalationspfad	Frist
Bias-Test-Mangel RecruitAI	Feststellung Auditor Hagedorn	CCO → CIO → CEO	Sofort (eskaliert am 28.02.2026)
BaFin-Anfrage CreditVision	Eingang 10.03.2026	CCO → CFO → CEO, extern Borchmann	15.05.2026

Risiko	Auslöser	Eskalationspfad	Frist
BR-Blockade Rollout	BR-Schreiben 05.01.2026	CCO → CEO → Einigung oder LAG	Dringend
OpenAI-Doku fehlt	CDO-Meldung 15.02.2026	CDO → CCO → Vendor-Eskalation	30.04.2026
DPIA nicht fristgerecht	LfDI-Aufforderung 02.03.2026	DSB → CCO → CEO	30.06.2026

5. Pflichten begrenztes Risiko (ServiceBot, PredictMaint, CodeAssist)

Für Systeme mit begrenztem Risiko gelten folgende Mindestanforderungen:

Anforderung	Grundlage	Status
Eintrag KI-Inventar	Interne Leitlinie	Erledigt
Transparenz-Hinweis (ServiceBot)	Art. 50 Abs. 1 KI-VO	Umgesetzt seit 01.02.2025
Kennzeichnung KI-Inhalte (CodeAssist)	Art. 50 Abs. 2 KI-VO	Prüfung läuft
Datenschutzprüfung	DSB-Empfehlung	Erledigt
Jährliche Überprüfung	Interne Leitlinie	Geplant Q4 2026

Aktenzeichen: TI-KI-2026-009. Verfasser: A. Kühnhausen, Dr. F. Roosendaal. Stand: März 2026.

Datei: 05-ai-literacy-curriculum.md

AI-Literacy-Curriculum und Schulungsplan — Art. 4 KI-VO

Aktenzeichen: TI-KI-2026-010

Dokumentversion: 1.3

Erstellungsdatum: 15. November 2025

Verfasser: Dr. Falk Roosendaal; Petra Schöneberger (Leiterin Personalentwicklung)

Zielgruppe: Alle Mitarbeiterinnen und Mitarbeiter der Thalheim Industries SE

1. Rechtsgrundlage und Zielsetzung

Art. 4 der Verordnung (EU) 2024/1689 (KI-VO) (<https://dejure.org/gesetze/KIVO/4.html>) verpflichtet Anbieter und Betreiber von KI-Systemen, dafür zu sorgen, dass ihr Personal und alle anderen Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ausreichende KI-Kompetenz verfügen, wobei technische Kenntnisse, Erfahrung, Ausbildung und Schulung sowie der Kontext berücksichtigt werden, in dem die KI-Systeme eingesetzt werden sollen.

Die Pflicht nach Art. 4 KI-VO gilt für Thalheim Industries SE als Betreiber (Deployer) aller fünf klassifizierten KI-Systeme. Sie ist spätestens ab 02.08.2025 anwendbar (Art. 113 Abs. 2 KI-VO).

Ziele des Schulungsprogramms:

1. Sicherstellen, dass alle Mitarbeiterinnen und Mitarbeiter die grundlegenden Funktionsweisen, Risiken und Rechte im Zusammenhang mit KI verstehen.
2. Schaffen zielgruppenspezifischer Vertiefungskennntnisse für Nutzer von Hochrisiko-Systemen.
3. Befähigung zur Wahrnehmung menschlicher Aufsicht über KI-Systeme (Art. 14 KI-VO).
4. Sensibilisierung für Hinweisgeberpflichten bei Anomalien oder Missbrauch.

2. Schulungsmatrix und Zielgruppen

Zielgruppe	Modul	Dauer	Format	Frist
Alle Mitarbeitenden	Modul A: KI-Grundlagen & Rechte	90 Min.	E-Learning	31.10.2026
Führungskräfte	Modul B: KI-Governance & Compliance	180 Min.	Hybrid (Präsenz + E-Learning)	31.07.2026
HR-Fachbereich	Modul C: RecruitAI — Hochrisiko & Bias	240 Min.	Präsenz-Workshop	31.05.2026
Finanzierung/Vertrieb	Modul D: CreditVision Score — KI-VO & DSGVO	240 Min.	Präsenz-Workshop	31.05.2026
IT / CDO-Bereich	Modul E: KI-Sicherheit, Protokollierung, Cybersecurity	120 Min.	E-Learning + Lab	30.06.2026
Compliance/Recht	Modul F: KI-VO Vertiefung für Compliance-Verantwortliche	360 Min.	Präsenz-Seminar extern	30.04.2026
Betriebsrat	Modul G: Mitbestimmung und KI (§ 87 BetrVG)	120 Min.	Externe Schulung	30.04.2026
Revision / Audit	Modul H: KI-Audit-Methodik	240 Min.	Externes Seminar	30.06.2026

3. Modulinhalte (Auszug)

Modul A — KI-Grundlagen & Rechte (Pflichtmodul für alle)

Lernziele:

- Was ist ein KI-System? (Art. 3 Nr. 1 KI-VO)
- Welche KI-Systeme setzt Thalheim ein und warum?
- Rechte betroffener Personen (Erklärung, Widerspruch, Art. 22 DSGVO)
- Verbotene KI-Praktiken nach Art. 5 KI-VO
- Meldewege bei Verdacht auf Missbrauch (Hinweisgeberschutz)
- Was ist Schatten-KI und warum ist sie problematisch?

Inhalte (Kurzübersicht):

1. Geschichte und Grundprinzipien der KI (15 Min.)
2. Überblick KI-Systeme bei Thalheim (10 Min.)
3. KI-Verordnung — Warum reguliert die EU? (20 Min.)
4. Ihre Rechte als betroffene Person (15 Min.)
5. Ihre Pflichten als Nutzer von KI-Systemen (15 Min.)
6. Quiz und Zertifizierung (15 Min.)

Modul C — RecruitAI: Hochrisiko und Bias (HR-Fachbereich)

Zielgruppe: HR-Business-Partner, Recruiterinnen und Recruiter, HR-Systemverantwortliche

Lernziele:

- Warum ist RecruitAI ein Hochrisiko-System (Anhang III Nr. 4a KI-VO)?
- Was bedeutet menschliche Aufsicht in der Praxis? (Art. 14 KI-VO)
- Bias-Erkennung: Wie entstehen Verzerrungen und wie erkenne ich sie?
- Recht auf Erklärung für Bewerber (Art. 22 DSGVO, DSGVO-Informationspflichten)
- SOP: Wann und wie überstimme ich das System?
- Dokumentationspflichten: Protokollierung von Override-Entscheidungen

Praxisübung: Fallstudie: RecruitAI bewertet eine Bewerberin mit niedrigem Score. Wie gehe ich vor? Rollenspiel zwischen HR-Partner und Kandidatin.

Modul D — CreditVision Score: KI-VO und DSGVO (Finanzierung/Vertrieb)

Zielgruppe: Kreditentscheider, Key Account Manager, Fachleiter Finanzierung

Lernziele:

- Hochrisiko-Klassifikation CreditVision Score (Anh. III Nr. 5b KI-VO)
- Art. 22 DSGVO: Wann liegt eine automatisierte Einzelentscheidung vor?
- Widerspruchsrecht des Kunden: wie kommunizieren, wie dokumentieren?
- Menschliche Aufsicht: Der Letztentscheid liegt beim Kundenbetreuer
- BaFin-Anfrage: Was bedeutet das für den Vertrieb?

4. Umsetzungsstand (März 2026)

Modul	Berechtigte Personen	Abgeschlossen	Prozentsatz
Modul A (Grundlagen)	12.000	4.560	38 %
Modul B (Führungskräfte)	480	210	44 %
Modul C (HR/RecruitAI)	85	31	36 %
Modul D (Finanzierung)	120	48	40 %
Modul E (IT)	340	198	58 %
Modul F (Compliance)	18	14	78 %
Modul G (Betriebsrat)	35	0	0 %
Modul H (Revision)	12	0	0 %

Bewertung: Der Umsetzungsstand ist kritisch. Im Bereich HR (Modul C) und Finanzierung (Modul D) — also genau den Fachbereichen mit Hochrisiko-Systemen — liegt die Abschlussquote unter 40 %. Modul G (Betriebsrat) wurde noch nicht gestartet, da die Schulung im Zusammenhang mit den laufenden Betriebsvereinbarungsverhandlungen steht.

5. Maßnahmenplan zur Schließung des Schulungsrückstands

Maßnahme	Verantwortlich	Frist	Erwartete Wirkung
Pflichtabschluss Modul A für alle (Erinnerungskampagne, Vorgesetzte eingebunden)	Personalentwicklung	30.06.2026	+45 %-Punkte
Präsenz-Workshops Modul C (3 Termine à 30 Teilnehmer)	HR / Dr. Roosendaal	31.05.2026	HR-Quote auf 100 %
Präsenz-Workshops Modul D (2 Termine)	Finanzierung / CCO	31.05.2026	Finanzierungs-Quote auf 100 %
Modul G: BR-Schulung nach Abschluss BV-Verhandlungen	CCO / Betriebsrat	31.07.2026	BR informiert und zertifiziert
Nachweis-Tracking im LMS (Lernmanagementsystem)	IT / PE	Laufend	Lückenlose Dokumentation
Eskalation bei Nicht-Abschluss an direkte Führungskraft	PE / Vorstand	Ab 01.05.2026	Steigerung Abschlussrate

6. Dokumentation und Nachweis

Die Schulungsabschlüsse werden im unternehmensinternen Lernmanagementsystem (LMS) TalentHub dokumentiert. Zertifikate werden automatisch ausgestellt. Die Compliance-Abteilung kann jederzeit aggregierte Nachweise je Fachbereich und System abrufen. Bei behördlichen Anfragen (BaFin, LfDI BW) können entsprechende Nachweise innerhalb von 72 Stunden bereitgestellt werden.

Aktenzeichen: TI-KI-2026-010. Verfasser: Dr. F. Roosendaal, P. Schöneberger. Stand: März 2026.

Datei: 06-vendor-due-diligence-openai.md

Vendor Due Diligence — OpenAI Ireland Ltd. / CodeAssist

Aktenzeichen: TI-KI-2026-011

Dokumentversion: 1.1

Erstellungsdatum: 05. Februar 2026

Verfasser: Marcus Petersen (CDO); Annegret Kühnhausen (CCO)

Status: Offene Punkte; Nachforderung an OpenAI Ireland Ltd. verschickt 15.02.2026

1. Hintergrund

Thalheim Industries SE setzt im Bereich Software-Entwicklung das Tool **CodeAssist** ein, das auf dem Sprachmodell GPT-4o von OpenAI Ireland Ltd. basiert. Der Vertrag besteht seit Juli 2024 (Enterprise-Lizenz, Vertragsnummer OAI-ENT-2024-TI-0892). CodeAssist ist im KI-Inventar als System mit begrenztem Risiko (GPAI-Modell, Art. 51 ff. KI-VO) klassifiziert.

Als Betreiber (Deployer) nach Art. 3 Nr. 4 KI-VO ist Thalheim Industries SE verpflichtet, sicherzustellen, dass das eingesetzte KI-System den Anforderungen der KI-VO entspricht. OpenAI Ireland Ltd. ist als Anbieter (Provider) des Basismodells nach Art. 53 KI-VO verpflichtet, folgende Pflichten zu erfüllen:

- Erstellung und Pflege technischer Dokumentation (Art. 53 Abs. 1 lit. a KI-VO);
- Einhaltung geltenden Urheberrechts (Art. 53 Abs. 1 lit. c KI-VO);
- Bereitstellung einer Zusammenfassung der Trainingsdaten (Art. 53 Abs. 1 lit. d KI-VO);
- Für Systeme mit systemischem Risiko: Meldepflichten, Adversarial Tests (Art. 55 KI-VO).

2. Prüfgegenstand

Im Rahmen der Due Diligence wurden folgende Themenbereiche untersucht:

Prüfbereich	Prüffrage	Ergebnis
Technische Dokumentation (Art. 11 / Art. 53 KI-VO)	Vollständige technische Dok. für CodeAssist vorgelegt?	**Nicht vollständig**
Datenschutz / Auftragsverarbeitung	AVV (DSGVO Art. 28) abgeschlossen?	Ja — OAI-DPA-2024-TI

Prüfbereich	Prüffrage	Ergebnis
Drittlandübermittlung	Verarbeitung in der EU sichergestellt (EEA-Verarbeitungsoption)?	Ja (EU-Data-Residency aktiv)
Nutzungsbedingungen / AUP	Entspricht Nutzung den OpenAI-Acceptable-Use-Policies?	Ja — geprüft
Incident Response	OpenAI-Sicherheitsvorfallmeldungen an Thalheim klar geregelt?	Teilweise — SLA unklar
KI-VO-Compliance-Seite OpenAI	Liegt produktspezifische EU-AI-Act-Konformitätserklärung vor?	**Nicht produktspezifisch**
Urheberrecht / IP	Code-Output-IP-Regelung vertraglich klar?	Ja — Vertrag §§ 6–8
Cybersicherheit	SOC 2 Type II vorliegend?	Ja (aktuell, gültig bis 11/2026)

3. Festgestellte Mängel

Mangel 1 — Fehlende produktspezifische technische Dokumentation

OpenAI hat auf Thalheims Anfrage (Schreiben CDO Petersen, 20.01.2026) lediglich auf die allgemeine EU-AI-Act-Compliance-Seite (<https://openai.com/eu-ai-act>) verwiesen. Diese enthält keine produktspezifischen Informationen zu CodeAssist als Deployment-Szenario für Thalheim. Insbesondere fehlen:

- Angaben zu den Trainings- und Testdaten-Parametern (Art. 53 Abs. 1 lit. d KI-VO);
- Dokumentation der implementierten Sicherheitsmechanismen;
- Angaben zu bekannten Schwächen des Modells (Known Limitations, Bias-Disclosure).

Die Anforderungen nach Art. 53 Abs. 1 lit. a und d KI-VO sind für Anbieter von Allzweck-KI-Modellen (GPAI-Modelle) verbindlich. OpenAI Ireland Ltd. ist als Anbieter des GPT-4o-Modells ein GPAI-Modell-Anbieter im Sinne von Art. 3 Nr. 63 KI-VO. Die Tatsache, dass ein generischer Compliance-Link bereitgestellt wird, genügt den Anforderungen nicht.

Bewertung: Kritischer Mangel. Nachforderung erforderlich.

Mangel 2 — Unklare SLA für Security-Incident-Meldungen

Der bestehende Vertrag (OAI-ENT-2024-TI-0892, Section 9) enthält keine spezifischen SLA-Klauseln zu den Fristen für Sicherheitsvorfallmeldungen, die KI-spezifische Risiken betreffen. Nach Art. 73 KI-VO sind Betreiber verpflichtet, schwerwiegende Vorfälle innerhalb von 15 Tagen (bei Todesfällen: sofort) an die nationale Marktüberwachungsbehörde zu melden. Dazu muss der Vendor unverzüglich informieren.

Bewertung: Mittlerer Mangel. Vertragsergänzung erforderlich.

4. Nachforderungsschreiben (zusammengefasst)

Mit Schreiben vom 15. Februar 2026 (CDO Petersen, Ref. TI-CDO-2026-0041) hat Thalheim OpenAI Ireland Ltd. folgende Unterlagen angefordert:

1. Produktspezifische technische Dokumentation für den Einsatz von GPT-4o in CodeAssist-Deployment-Szenarios nach Art. 53 KI-VO;
2. Zusammenfassung der Trainingsdatenbasis des eingesetzten Modells;
3. Disclosure bekannter Schwächen (Halluzinierungsrate, Bias-Kategorie);
4. Ergänzende Vereinbarung zu Sicherheitsvorfallmeldungen (Incident Notification SLA max. 24 h);
5. Klarstellung, ob GPT-4o als GPAI-Modell mit systemischem Risiko eingestuft ist (Art. 51 KI-VO).

Antwortfrist: 30. April 2026.

5. Handlungsempfehlungen

Empfehlung	Priorität	Frist
Eskalation bei OpenAI auf Enterprise-Account-Manager-Ebene	Hoch	Sofort
Prüfung alternativer Vendor-Optionen für KI-Coding-Assistent (z. B. GitHub Copilot, Anthropic Claude)	Mittel	30.06.2026
Vertragsergänzung: Incident Notification SLA, EU-AI-Act-Klausel	Hoch	30.04.2026
Interne Nutzungsrichtlinie CodeAssist aktualisieren: keine personenbezogenen Daten, keine geheimen Informationen in Prompts	Hoch	28.02.2026 ✓ (erledigt)
AI Literacy Schulung IT-Personal (Modul E) priorisieren	Mittel	30.06.2026

6. Vendor-Risikobewertung (Gesamt)

Kriterium	Bewertung	Begründung
Datenschutz-Compliance	Gut	AVV vorhanden, EEA-Residency aktiv
KI-VO-Dokumentation	**Unzureichend**	Keine produktspezifische Doku
Finanzielle Stabilität	Sehr gut	OpenAI valide Marktkapitalisierung
Vertragliche KI-VO-Klauseln	Ausbaubar	Nachverhandlung erforderlich

Kriterium	Bewertung	Begründung
Cybersicherheit	Gut	SOC 2 Type II aktuell
Gesamtrisiko	**Mittel**	Doku-Mangel behebbar, aber fristkritisch

Aktenzeichen: TI-KI-2026-011. Verfasser: M. Petersen, A. Kühnhausen. Stand: März 2026.

Datei: 07-dpia-recruiting-tool.md

Datenschutz-Folgenabschätzung (DPIA) — RecruitAI

Aktenzeichen intern: TI-KI-2026-012

Behördliches AZ: LfDI BW AZ 1-1085.51/2026/045

Dokumentversion: 0.8 (Entwurf, nicht freigegeben)

Erstellungsdatum: 10. März 2026

Verfasserin: Dr. Carla Eichenmüller, Datenschutzbeauftragte Thalheim Industries SE

Mitarbeit: Barbara Trenkmann (HR-Systemverantwortliche); Marcus Petersen (CDO)

Vorlage-Frist: 30. Juni 2026 (gemäß LfDI BW Schreiben 02.03.2026)

1. Einleitung und Rechtsgrundlage

Die Thalheim Industries SE ist gemäß Art. 35 Abs. 1 und Abs. 3 DSGVO (<https://dejure.org/gesetze/DSGVO/35.html>) verpflichtet, für die Verarbeitung personenbezogener Daten mittels des KI-Systems **RecruitAI** (Vendor: Synaptec Analytics GmbH) eine Datenschutz-Folgenabschätzung (DPIA) durchzuführen.

Die DPIA-Pflicht ergibt sich aus:

- Art. 35 Abs. 3 lit. a DSGVO: Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen durch automatisierte Verarbeitung einschließlich Profiling mit erheblichen Folgen für die betroffene Person → Bewerber-Ranking mit Einstellungsrelevanz.
- Art. 35 Abs. 3 lit. b DSGVO: Umfangreiche Verarbeitung besonderer Kategorien von Daten (Art. 9 DSGVO) — nicht ausgeschlossen (Rückschlüsse auf Herkunft, Geschlecht aus Lebensläufen).
- LfDI BW Positivliste: Automatisierte Entscheidungsunterstützung im Recruiting ausdrücklich aufgeführt.
- KI-VO-Synergiegebot: Art. 9 KI-VO und Art. 35 DSGVO sollen koordiniert angewendet werden (Erwägungsgrund 159 KI-VO).

Das Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) hat mit Schreiben vom 02.03.2026 (AZ 1-1085.51/2026/045) die Vorlage der vollständigen DPIA bis 30.06.2026 angefordert.

2. Systembeschreibung

Merkmal	Inhalt
Systemname	RecruitAI
Anbieter	Synaptec Analytics GmbH, Leopoldstraße 18, 80802 München
Einsatz seit	01. September 2024
Einsatzzweck	Automatisiertes Screening und Ranking von Bewerbungsunterlagen für alle Stellenausschreibungen der Thalheim Industries SE
Datenkategorien	Name, Vorname, Kontaktdaten, Lebenslauf, Zeugnisse, Foto (falls beigefügt), Anschreiben, LinkedIn-Profil (optionale Verknüpfung)
Betroffene Personen	Bewerberinnen und Bewerber (extern), durchschnittlich 4.500 Bewerbungen p.a.
Entscheidungstiefe	Ranking-Score 0–100; Schwelle 65 für automatische Weiterleitung; unter 40 automatische Ablehnung möglich (Override durch HR vorgesehen)
Datenspeicherung	Synaptec-Server (EU, Frankfurt a.M.); Aufbewahrung: 6 Monate nach Abschluss Stellenbesetzung
Schnittstellen	SAP SuccessFactors (ATS), Outlook (Kommunikation), Active Directory

3. Beschreibung des Verarbeitungsvorgangs

Verarbeitungsschritte:

1. Eingang der Bewerbungsunterlagen über das Thalheim-Karriereportal oder E-Mail.
2. Automatische Extraktion strukturierter Daten (CV-Parsing): Berufserfahrung, Ausbildung, Skills, Sprachkenntnisse.
3. Scoring durch das RecruitAI-Modell: Vergleich der Kandidatenprofil-Vektoren mit einem Job-Requirement-Profil (erstellt durch HR-Business-Partner).
4. Ranking-Ergebnis: Score-Liste aller Kandidaten für die Stelle.
5. HR-Business-Partner sieht Ranking, kann manuell überstimmen (Override), gibt Bewerbungen in die nächste Runde.
6. Kandidaten unter Schwelle 40: automatische Ablehnungsmail — **kritischer Punkt für Art. 22 DSGVO**.

4. Notwendigkeit und Verhältnismäßigkeit

Zweck: Effiziente Bewältigung hoher Bewerbungsvolumina (4.500 p.a.) bei gleichzeitiger Sicherung einheitlicher Qualitätsstandards.

Verhältnismäßigkeit: Das System ist grundsätzlich geeignet und erforderlich. Kritisch ist jedoch die automatische Ablehnung unterhalb der Schwelle 40, die einen Fall von Art. 22 Abs. 1 DSGVO (<https://dejure.org/gesetze/DSGVO/22.html>) darstellen kann, wenn kein HR-Mensch aktiv eingreift. Synaptec behauptet, dass jede Ablehnungsentscheidung technisch von HR bestätigt werden muss — dies ist jedoch in der Praxis nicht vollständig implementiert (Feststellung Hagedorn-Audit, 28.02.2026).

5. Risikoidentifikation und -bewertung

Risiko	Wahrscheinlichkeit	Schwere	Risikostufe	Maßnahme
Bias / Diskriminierung (Geschlecht, Herkunft)	Mittel	Hoch	**Hoch**	Bias-Tests erforderlich (fehlen derzeit)
Automatische Ablehnung ohne menschliche Kontrolle	Mittel	Hoch	**Hoch**	SOP und technische Sperre erforderlich
Fehlende Transparenz gegenüber Bewerbern	Hoch	Mittel	**Hoch**	Datenschutzhinweis aktualisieren
Datenpanne (Synaptec-Server)	Niedrig	Hoch	Mittel	AVV, Pen-Test, ISO 27001 Synaptec
Profilbildung / Scope Creep	Niedrig	Mittel	Niedrig	Datenminimierungspflicht vertraglich
Rückschlüsse auf Sonderkategorien (Art. 9 DSGVO)	Mittel	Sehr hoch	**Hoch**	Filterung besonderer Kategorien technisch

6. Konsultation des Datenschutzbeauftragten

Dr. Eichenmüller wurde als Datenschutzbeauftragte gemäß Art. 35 Abs. 2 DSGVO bereits zu Beginn der DPIA eingebunden. Sie hat die Risikoidentifikation begleitet und empfiehlt die vollständige Implementierung aller Maßnahmen aus Abschnitt 5, bevor RecruitAI im Vollbetrieb verbleibt. Sie empfiehlt außerdem, eine Konsultation des LfDI BW nach Art. 36 DSGVO zu prüfen, falls die Risiken nicht vollständig eingedämmt werden können (Bias-Tests ausstehend).

7. Offene Punkte (Stand: März 2026)

Offener Punkt	Verantwortlich	Frist
Bias-Tests Synaptec — Durchführung und Dokumentation	Synaptec / CIO Wolfsbacher	30.05.2026
Technische Sperre: keine Ablehnung ohne aktiven HR-Override	IT / Synaptec	30.04.2026
Aktualisierung Datenschutzhinweis Karriereportal (Art. 13 DSGVO)	DSB / HR	31.03.2026

Offener Punkt	Verantwortlich	Frist
Überarbeitung Kandidaten-Kommunikation: Hinweis KI-gestütztes Screening	HR / Kommunikation	31.03.2026
Überprüfung AVV mit Synaptec (neue KI-VO-Klauseln)	DSB / Legal	30.04.2026
Abschluss DPIA-Bericht und Einreichung LfDI BW	DSB Dr. Eichenmüller	30.06.2026

Aktenzeichen: TI-KI-2026-012. LfDI BW: AZ 1-1085.51/2026/045. Verfasserin: Dr. C. Eichenmüller. Entwurf v0.8, Stand März 2026.

Datei: 08-incident-response-playbook.md

KI-Incident-Response-Playbook — Thalheim Industries SE

Aktenzeichen: TI-KI-2026-013

Dokumentversion: 1.0

Freigegeben durch: CCO Annegret Kühnhausen; CIO Dr. Sigrid Wolfsbacher

Freigabedatum: 01. März 2026

Geltungsbereich: Alle KI-Systeme im KI-Inventar der Thalheim Industries SE

1. Zweck und Anwendungsbereich

Dieses Playbook definiert den konzernweiten Prozess zur Erkennung, Klassifikation, Reaktion und Meldung von KI-bezogenen Sicherheits- und Compliance-Vorfällen (KI-Incidents). Es ergänzt das bestehende allgemeine IT-Incident-Response-Framework (IT-IRM-2024) und das Datenschutzverletzungs-Protokoll nach Art. 33/34 DSGVO.

Rechtsgrundlagen:

- Art. 73 KI-VO: Meldung schwerwiegender Vorfälle an Marktüberwachungsbehörde (<https://dejure.org/gesetze/KIVO/73.html>)
- Art. 33 DSGVO: Meldung von Datenschutzverletzungen an Aufsichtsbehörde (<https://dejure.org/gesetze/DSGVO/33.html>)
- Art. 26 Abs. 4 KI-VO: Betreiberpflicht zur Incident-Meldung

2. Incident-Klassifikation

Klasse 1 — Kritisch (Sofortmaßnahmen erforderlich)

Definition: Schwerwiegender Vorfall nach Art. 3 Nr. 49 KI-VO, der eine ernsthafte Bedrohung für Gesundheit, Sicherheit oder Grundrechte darstellt oder zu einem Todesfall geführt hat oder hätte führen können.

Beispiele bei Thalheim:

- RecruitAI lehnt systematisch alle Bewerber einer bestimmten Nationalität ab (Diskriminierungsverdacht)
- CreditVision Score weist nachweisbaren Bias gegen bestimmte Bevölkerungsgruppen auf
- Datenpanne bei Synaptec: Bewerberdaten öffentlich zugänglich

Reaktionspflicht: Sofortiger Stopp des Systems + Meldung an BNetzA (Art. 73 KI-VO) binnen 15 Tagen (Todesfall: sofort).

Klasse 2 — Schwerwiegend (Reaktion binnen 24 Stunden)

Definition: Fehlfunktion mit erheblichem Schaden für einzelne Personen; Compliance-Verstoß der KI-VO mit behördlichem Korrekturpotenzial.

Beispiele:

- RecruitAI generiert Score-Ausgaben jenseits des 0–100-Rahmens (Systemfehler)
- CodeAssist gibt Code mit kritischen Sicherheitslücken aus, der ungeprüft in Produktion überführt wird
- Schatten-KI in einem Fachbereich mit Personenbezug entdeckt (vgl. Strang 7)

Reaktionspflicht: CCO + CIO informieren, System isolieren, Sachverhaltsklärung, ggf. LfDI BW.

Klasse 3 — Moderat (Reaktion binnen 72 Stunden)

Definition: Funktionsstörungen ohne unmittelbaren Personenschaden; Verstöße gegen interne Richtlinien.

Beispiele:

- Unberechtigter Zugriff auf Recruiting-Daten intern (Mitarbeiter ohne Berechtigung)
- ServiceBot gibt falsche Produktinformationen an Kunden aus
- PredictMaint empfiehlt Wartungsintervalle mit erheblicher Abweichung (wirtschaftlicher Schaden)

Reaktionspflicht: CDO + IT-Security; Dokumentation; ggf. Kundenbenachrichtigung.

Klasse 4 — Gering (Reaktion binnen 1 Woche)

Definition: Qualitätsprobleme, Leistungsabfälle, Nutzerbeschwerden ohne Rechtsverletzung.

Beispiele:

- CodeAssist-Antwortqualität sinkt nach Modell-Update
- Bewerbungsportal-Chatbot versteht Fachjargon nicht

Reaktionspflicht: CDO, Ticketsystem, regulärer Betrieb.

3. Incident-Response-Prozess

Schritt 1: Erkennung und Meldung

Erkennungsquellen:

- Automatische Monitoring-Alarme (KI-Dashboard, CDO-Bereich)
- Meldungen von Mitarbeitenden (Hinweisgebersystem, intern: ki-incident@thalheim.de)
- Kundenbeschwerden (Vertrieb, Kundenservice)
- Behördliche Anfragen (BaFin, LfDI BW)
- Revisionsfeststellungen (interne Revision, Hagedorn & Partner)

Erstmeldung: Jede Mitarbeiterin und jeder Mitarbeiter, der einen KI-Incident erkennt oder vermutet, ist verpflichtet, diesen unverzüglich über das interne Meldeformular (ki-incident@thalheim.de) oder mündlich an den IT-Service-Desk (intern: 4-4000) zu melden.

Schritt 2: Erstklassifikation (ICO on Duty)

Der CDO oder sein Stellvertreter klassifiziert den Vorfall innerhalb von 2 Stunden nach Erstmeldung (Klasse 1–4). Bei Klasse 1 und 2: sofortige Eskalation an CCO, CIO, ggf. CEO.

Schritt 3: Sofortmaßnahmen

Klasse	Sofortmaßnahme	Verantwortlich
1	System stoppen; Notfallteam einberufen; Behörden informieren	CCO + CIO + CEO
2	System isolieren; Sachverhaltsklärung; Behörden nach 24h	CCO + CIO
3	Diagnose; ggf. System einschränken; Bericht in 72h	CDO + IT-Security
4	Ticket; Analyse; reguläres Verfahren	CDO

Schritt 4: Behördliche Meldepflichten

Behörde	Pflicht	Frist	Voraussetzung
Bundesnetzagentur (BNetzA)	Art. 73 KI-VO — schwerwiegender Vorfall	15 Tage ab Kenntnis	Klasse-1-Vorfall Hochrisiko-System
LfDI BW	Art. 33 DSGVO — Datenschutzverletzung	72 Stunden	Datenpanne mit Risiko für Betroffene
BaFin	MaRisk / aufsichtsrechtlich	Nach MaRisk	CreditVision Score — Systemversagen

Zuständig für alle Behördenmeldungen: CCO Annegret Kühnhausen in Abstimmung mit Kanzlei Borchmann Compliance.

Schritt 5: Ursachenanalyse und Abschlussbericht

Innerhalb von 30 Tagen nach Incident-Schließung erstellt das CDO-Büro einen Abschlussbericht mit Root-Cause-Analyse und Maßnahmen zur Vermeidung von Wiederholungen. Der Bericht fließt in die jährliche KI-Governance-Review ein.

4. Spezialfall: Schatten-KI (nicht genehmigte Systeme)

Der Vorfall in der Marketingabteilung (identifiziert März 2026 durch Konzernrevision) zeigt, dass Schatten-KI als eigenständige Incident-Klasse zu behandeln ist:

Vorgehen bei Schatten-KI-Entdeckung:

1. Sofortige Abschaltung des nicht genehmigten Systems durch IT auf Anweisung CDO.
2. Sicherung der Nutzungsprotokolle (soweit zugänglich).
3. Datenschutzprüfung: Wurden personenbezogene Daten verarbeitet? → DSGVO Art. 33?
4. Disziplinarische Anhörung der verantwortlichen Person (Personalrecht, CCO + HR).
5. Analyse: Wie konnte das System eingesetzt werden? Technische Zugangskontrollen verschärfen.
6. Protokollierung im Incident-Register.

5. Incident-Register

Alle KI-Incidents werden im zentralen KI-Incident-Register (SharePoint, Zugriff: CCO, CDO, CIO, DSB) dokumentiert mit folgenden Feldern:

- Incident-ID; Datum; Klasse; betroffenes System; Beschreibung; Entdeckungsquelle; Sofortmaßnahmen; Behördliche Meldungen; Root Cause; Abschlussdatum; Maßnahmen.

Aktueller Eintrag:

- INC-2026-003: Schatten-KI Marketing (Midjourney-API); entdeckt 14.03.2026; Klasse 2; IT-Abschaltung 14.03.2026; Sachverhaltsklärung läuft.

Aktenzeichen: TI-KI-2026-013. Freigegeben: A. Kühnhausen, Dr. S. Wolfsbacher. Stand: März 2026.

Datei: 09-rote-listen-verbotene-praktiken.md

Rote Liste — Verbotene KI-Praktiken nach Art. 5 KI-VO

Aktenzeichen: TI-KI-2026-013

Dokumentversion: 1.1

Erstellungsdatum: 20. Dezember 2025

Verfasser: Annegret Kühnhausen (CCO); Kanzlei Borchmann Compliance (Frankfurt)

Geltungsbereich: Alle Mitarbeiterinnen und Mitarbeiter, Führungskräfte, Auftragnehmer

1. Zweck und Verpflichtung

Art. 5 der Verordnung (EU) 2024/1689 (KI-VO) (<https://dejure.org/gesetze/KIVO/5.html>) enthält eine abschließende Liste von KI-Praktiken, die in der Europäischen Union verboten sind. Diese Verbote gelten seit dem 02. Februar 2025 (Art. 113 Abs. 1 KI-VO).

Thalheim Industries SE hat als Betreiber (Deployer) und in Teilen als Anbieter (Provider — insbesondere für intern entwickelte Systeme wie PredictMaint und ServiceBot) sicherzustellen, dass keine der nachfolgend aufgeführten verbotenen Praktiken eingesetzt oder gefördert wird. Verstöße können mit Bußgeldern von bis zu 35 Mio. EUR oder 7 % des globalen Jahresumsatzes belegt werden (Art. 99 Abs. 3

KI-VO).

Diese Rote Liste ist für alle Beschäftigten und Führungskräfte verbindlich. Sie ergänzt die KI-Governance-Leitlinie (Aktenstück 01) und ist in das AI-Literacy-Curriculum (Aktenstück 05, Modul A) integriert.

2. Verbotene Praktiken (Art. 5 KI-VO) — Vollständige Übersicht

2.1 Unterschwellige Beeinflussung (Art. 5 Abs. 1 lit. a KI-VO)

Verboten: Das Inverkehrbringen, die Inbetriebnahme oder Verwendung von KI-Systemen, die durch Techniken der unterschwelligen Beeinflussung, die von einer Person nicht wahrgenommen werden können, das Verhalten dieser Person in einer Weise beeinflussen, die dazu bestimmt ist oder die Wirkung hat, ihr oder einer anderen Person erheblichen Schaden zuzufügen.

Praxisrelevanz Thalheim: KEIN Thalheim-System fällt aktuell unter diesen Tatbestand. Mögliches Risiko: Marketing-Tools, die Nudging-Techniken einsetzen. Prüfpflicht bei Einführung neuer Marketing-KI.

Merke: Auch klassische Nudge-Algorithmen (E-Commerce-Empfehlungen) sind nur dann verboten, wenn sie unterschwellig und schädigend wirken.

2.2 Ausnutzung von Vulnerabilitäten (Art. 5 Abs. 1 lit. b KI-VO)

Verboten: KI-Systeme, die Vulnerabilitäten einer Person oder Gruppe ausnutzen, die auf Alter, Behinderung oder sozialer oder wirtschaftlicher Situation basieren.

Praxisrelevanz Thalheim: KEIN direktes Risiko bei aktuellen Systemen. Potenzielles Risiko: ServiceBot — wenn er vulnerable Kundengruppen (z. B. ältere Personen, wirtschaftlich benachteiligte Kunden) gezielt ausnutzt, um Vertragsabschlüsse zu erzielen.

Maßnahme: ServiceBot ist auf sachliche Kundeninformation beschränkt; keine Verkaufsstrategie auf Basis Kundenvulnerabilitäten.

2.3 Social Scoring (Art. 5 Abs. 1 lit. c KI-VO)

Verboten: KI-Systeme, die von öffentlichen Behörden (oder in deren Auftrag) zur Bewertung natürlicher Personen auf der Grundlage des Sozialverhaltens oder persönlicher Merkmale eingesetzt werden, mit nachteiligen Folgen.

Praxisrelevanz Thalheim: Nicht anwendbar (Thalheim ist keine Behörde). Jedoch: interne Mitarbeiterbewertungs-KI, die systematisch Verhaltensprofile erstellt und für Personalentscheidungen nutzt, könnte dem Geist dieser Vorschrift widersprechen und nach § 87 BetrVG mitbestimmungspflichtig sein.

2.4 Vorhersagebasierte Polizeiarbeit (Art. 5 Abs. 1 lit. d KI-VO)

Verboten: KI-Systeme für Risikoabschätzungen natürlicher Personen hinsichtlich der Begehung einer Straftat, ausschließlich auf der Grundlage von Profiling oder Persönlichkeitsmerkmalen.

Praxisrelevanz Thalheim: Nicht anwendbar.

2.5 Anlasslose biometrische Massenüberwachung (Art. 5 Abs. 1 lit. e KI-VO)

Verboten: Echtzeit-Fernerkennung biometrischer Merkmale in öffentlich zugänglichen Räumen durch Strafverfolgungsbehörden.

Praxisrelevanz Thalheim: Nicht anwendbar (Thalheim ist keine Strafverfolgungsbehörde). Jedoch: Kamerasysteme im Werksgelände, die Personen erkennen, sind sorgfältig zu prüfen.

2.6 Emotionserkennung (Art. 5 Abs. 1 lit. f KI-VO)

Verboten: KI-Systeme zur Erkennung von Emotionen am Arbeitsplatz und in Bildungseinrichtungen, außer aus medizinischen oder Sicherheitsgründen.

Praxisrelevanz Thalheim: HOCH. Jedes System, das Stimmungen, Emotionen oder den emotionalen Zustand von Mitarbeitern am Arbeitsplatz analysiert (z. B. Analyse von Videomeetings, Sprachanalyse in Call-Centern), ist in Deutschland nach Art. 5 Abs. 1 lit. f KI-VO VERBOTEN. Prüfung aller Call-Center-Systeme und Meeting-Analyse-Tools erforderlich.

Maßnahme: CCO hat Bestandsaufnahme laufender und geplanter HR-Analytics-Systeme angeordnet (Frist: 30.04.2026).

2.7 Biometrische Kategorisierung (Art. 5 Abs. 1 lit. g KI-VO)

Verboten: KI-Systeme, die biometrische Daten verwenden, um natürliche Personen nach politischen Ansichten, Gewerkschaftszugehörigkeit, Religion, Weltanschauung, Rasse, Sexualleben oder sexueller Ausrichtung zu kategorisieren.

Praxisrelevanz Thalheim: HOCH für Recruiting. RecruitAI darf nicht direkt oder indirekt Bewerber nach solchen Merkmalen kategorisieren. Die fehlenden Bias-Tests (Strang 1) erhöhen das Risiko, dass solche Kategorisierungen unbeabsichtigt im Modell abgebildet sind.

2.8 Biometrische Fernidentifikation in Echtzeit (Art. 5 Abs. 1 lit. h KI-VO)

Verboten: Echtzeit-Fernidentifikation biometrischer Merkmale in öffentlich zugänglichen Räumen durch Strafverfolgungsbehörden (mit engen Ausnahmen).

Praxisrelevanz Thalheim: Nicht anwendbar.

3. Prüfschema für neue KI-Systeme

Für jedes neue KI-System ist vor Einführung folgendes Prüfschema zu durchlaufen:

''' Schritt 1: Fällt das System unter Art. 5 Abs. 1 KI-VO (Verbote)? ■■ JA → Sofortiger Stopp. Keine Einführung. Meldung an CCO. ■■ NEIN → weiter mit Schritt 2.

Schritt 2: Fällt das System unter Art. 6 / Anh. III KI-VO (Hochrisiko)? ■■ JA → Vollständige Konformitätsprüfung vor Einsatz. KI-Clearance erforderlich. ■■ NEIN → weiter mit Schritt 3.

Schritt 3: Fallen Transparenzpflichten nach Art. 50 KI-VO an? ■■ JA → Hinweispflichten umsetzen. Freigabe durch CCO. ■■ NEIN → Eintrag KI-Inventar, jährliche Überprüfung. '''

4. Meldeverpflichtung

Jede Mitarbeiterin und jeder Mitarbeiter, die/der bemerkt oder vermutet, dass ein KI-System bei Thalheim eine verbotene Praktik umsetzt oder umgesetzt werden soll, ist verpflichtet, dies unverzüglich zu melden:

- Intern: ki-incident@thalheim.de oder CCO Kühnhausen direkt
- Extern: Hinweisgeberschutzgesetz (HinSchG) — externe Meldestelle (Bundesamt für Justiz)

Meldungen sind vertraulich und werden durch das Hinweisgeberschutzsystem des Unternehmens geschützt.

Aktenzeichen: TI-KI-2026-013. Verfasser: A. Kühnhausen, Kanzlei Borchmann. Stand: Dezember 2025.

Datei: 10-protokoll-ki-komitee-quartal1.md

Protokoll — KI-Komitee-Sitzung Q1 2026

Aktenzeichen: TI-KI-2026-014

Datum: 14. März 2026, 09:00–12:30 Uhr

Ort: Thalheim Industries SE, Sitzungszimmer Energiehalle (EG, Gebäude A), Mannheim

Protokollführer: Claudia Berger-Hentschel, Vorstandsassistentz

Anwesende

Person	Funktion	Anmerkung
Dr. Falk Roosendaal	KI-Komitee-Vorsitz	
Dr. Sigrid Wolfsbacher	CIO	
Marcus Petersen	CDO	
Annegret Kühnhausen	CCO	
Dr. Carla Eichenmüller	Datenschutzbeauftragte	
Barbara Trenkmann	Leiterin HR-Systeme	Gast zu TOP 2
Rolf Haselmann	Leiter Kundenfinanzierung	Gast zu TOP 3
Franz-Josef Brammer	Leiter Konzernrevision	Gast zu TOP 6
Dr. Nora Borchmann	Kanzlei Borchmann Compliance	Externer Gast

Entschuldigt: Prof. Dr. Schirrmeister (COO), Klaus-Dieter Obermaier (CFO)

Tagesordnung

1. Genehmigung Protokoll Q4 2025
2. RecruitAI: Statusbericht Konformitätsprüfung und Bias-Test-Mangel
3. CreditVision Score: BaFin-Anfrage — Sachstand und Handlungsoptionen
4. Betriebsvereinbarung KI: Verhandlungsstand Betriebsrat
5. AI Literacy: Schulungsfortschritt und Maßnahmenplan
6. Konzernrevision: Schatten-KI Marketing
7. OpenAI-Vendor: Nachforderungsstatus
8. Sonstiges

TOP 1 — Genehmigung Protokoll Q4 2025

Das Protokoll der Sitzung vom 10. Januar 2026 wird ohne Änderungen genehmigt. **Beschluss 2026-KI-001: Protokoll genehmigt.**

TOP 2 — RecruitAI: Statusbericht Konformitätsprüfung und Bias-Test-Mangel

Berichterstatterin: Barbara Trenkmann; Dr. Wolfsbacher

Trenkmann berichtet: Die externe Konformitätsprüfung durch Hagedorn & Partner (Audit-Start 15.01.2026) hat am 28.02.2026 einen Zwischenbericht vorgelegt. Kernergebnis: Synaptec Analytics GmbH hat keine dokumentierten Bias-Tests nach Art. 9 Abs. 7 KI-VO für das RecruitAI-Modell vorgelegt. Die entsprechende technische Dokumentation fehlt oder ist unvollständig.

Wolfsbacher ergänzt: Die CIO hat Synaptec mit Schreiben vom 05.03.2026 (Ref. TI-CIO-2026-0014) aufgefordert, bis 30.05.2026 vollständige Bias-Test-Berichte vorzulegen. Synaptec hat den Empfang bestätigt, jedoch keine Zusage zum Inhalt gemacht.

Dr. Borchmann (extern): Weist darauf hin, dass das Fehlen von Bias-Tests bei einem Hochrisiko-System nach Art. 9 Abs. 7 KI-VO ein schwerwiegender Mangel darstellt. Empfiehlt: Thalheim sollte parallel eigene Bias-Tests initiieren, um nicht vollständig von Synaptec abhängig zu sein. Kostenschätzung für externes Bias-Testing: 45.000–80.000 EUR.

Roosendaal: Schlägt vor, das Bias-Testing parallel sowohl durch Synaptec als auch durch einen unabhängigen Dritten durchzuführen. Einigkeit im Komitee.

Beschluss 2026-KI-002: CCO beauftragt bis 31.03.2026 einen unabhängigen Bias-Test-Dienstleister für RecruitAI. Budget: bis 80.000 EUR aus Governance-Reserve genehmigt.

Beschluss 2026-KI-003: Bis zum Vorliegen der Bias-Test-Ergebnisse wird RecruitAI mit erhöhter menschlicher Aufsicht betrieben: jede automatische Ablehnung bedarf einer aktiven Bestätigung durch HR-Business-Partner.

TOP 3 — CreditVision Score: BaFin-Anfrage

Berichterstatter: Rolf Haselmann; Annegret Kühnhausen; Dr. Borchmann

Kühnhausen berichtet: Mit Schreiben vom 10.03.2026 (GZ BJ 24-K 7102-2026/0012) hat die BaFin um Stellungnahme gebeten, ob (1) Art. 22 DSGVO beim Kreditscoring eingehalten wird und (2) eine interne Konformitätsbewertung nach Art. 43 Abs. 2 KI-VO für CreditVision Score vorliegt. Antwortfrist: 15.05.2026.

Haselmann: Im Prozess sei grundsätzlich eine menschliche Letztentscheidung vorgesehen, aber die SOPs seien nicht in allen Vertriebsstützpunkten konsequent dokumentiert. CreditVision AG hat technische Unterlagen erst teilweise geliefert.

Dr. Borchmann: Empfiehlt, die Stellungnahme an die BaFin durch die Kanzlei zu koordinieren. Inhaltlich sollte dargelegt werden: (1) Letztentscheid durch Menschen, (2) Informationspflichten gegenüber Kunden, (3) geplante vollständige Konformitätsbewertung bis 31.07.2026.

Beschluss 2026-KI-004: Kanzlei Borchmann Compliance koordiniert Stellungnahme an BaFin bis 12.05.2026. Haselmann liefert prozessbezogene Unterlagen bis 15.04.2026.

TOP 4 — Betriebsvereinbarung KI: Verhandlungsstand

Berichterstattein: Annegret Kühnhausen

Kühnhausen berichtet: Der Betriebsrat (Vorsitzender Norbert Schäpers) hat mit Schreiben vom 05.01.2026 und 20.02.2026 klargestellt, dass er dem Produktiveinsatz von RecruitAI und CreditVision Score ohne abgeschlossene Betriebsvereinbarung nach § 87 Abs. 1 Nr. 6 BetrVG (<https://dejure.org/gesetze/BetrVG/87.html>) nicht zustimmt.

Stand der Verhandlungen: Es haben drei Gespräche stattgefunden. Der BR fordert: (a) vollständige Transparenz über Algorithmus-Logik, (b) Recht auf externe Sachverständige, (c) regelmäßige Berichterstattung. Thalheim hat (a) und (c) prinzipiell zugestimmt, bei (b) steht die juristische Prüfung aus.

Roosendaal: Terminiert nächstes BR-Gespräch auf 08.04.2026. Ziel: Einigung auf BV-Grundstruktur bis Ende April.

Beschluss 2026-KI-005: Mediationsangebot an Betriebsrat für externes Moderationsverfahren. Wenn bis 31.05.2026 keine Einigung, prüft die CCO arbeitsrechtliche Optionen (Einigungsstelle nach § 76 BetrVG).

TOP 5 — AI Literacy: Schulungsfortschritt

Berichterstatter: Marcus Petersen

Petersen berichtet: Stand März 2026 haben 38 % aller Mitarbeitenden Modul A abgeschlossen. Im HR-Bereich (Modul C): 36 %. In der Finanzierung (Modul D): 40 %. Betriebsrat noch nicht geschult.

Komitee-Diskussion: Einigung, dass der Schulungsrückstand ein signifikantes Compliance-Risiko darstellt. Nachweispflicht nach Art. 4 KI-VO könnte bei behördlicher Anfrage nicht erfüllt werden.

Beschluss 2026-KI-006: Personalentwicklung erhält Direktive des Vorstands (Kühnhausen holt ab), alle Module bis 31.10.2026 vollständig abzuschließen. Führungskräfte werden für ihre Teams verantwortlich gemacht. Monatliches Reporting an KI-Komitee ab April 2026.

TOP 6 — Schatten-KI Marketing

Berichterstatter: Franz-Josef Brammer (Leiter Konzernrevision)

Brammer berichtet: Die Konzernrevision hat am 14.03.2026 festgestellt, dass die Marketingabteilung (Leiter: Dr. Philipp Sonntag) seit mindestens acht Monaten ein nicht im KI-Inventar registriertes GenAI-Tool (Midjourney in Verbindung mit einer eigenen API-Anbindung) für Bild- und Textgenerierung nutzt. Die Nutzung erfolgte ohne:

- Datenschutzprüfung (ob personenbezogene Daten verarbeitet wurden, ist noch unklar)
- Sicherheitsfreigabe (IT-Security)
- Eintrag im KI-Inventar
- Freigabe durch CCO oder CDO

Dr. Sonntag hat in der Anhörung angegeben, nicht gewusst zu haben, dass eine Freigabe erforderlich ist.

Kühnhausen: Das System wurde am 14.03.2026 durch IT abgeschaltet. Eine arbeitsrechtliche Anhörung läuft. Datenschutz-Prüfung durch DSB Eichenmüller: läuft.

Wolfsbacher: Technische Schutzmaßnahmen (Blocking nicht genehmigter API-Endpunkte) werden bis 30.04.2026 implementiert.

Beschluss 2026-KI-007: Konzernrevision erstellt vollständigen Revisionsbericht (Aktenstück 16) bis 30.04.2026. Alle Fachbereiche werden angewiesen, bis 15.04.2026 alle verwendeten KI-Tools zu melden.

TOP 7 — OpenAI-Vendor: Nachforderungsstatus

Berichterstatter: Marcus Petersen

Petersen berichtet: Nachforderungsschreiben vom 15.02.2026 ist versendet. Keine Antwort von OpenAI Ireland bis heute. Antwortfrist 30.04.2026. Enterprise Account Manager wurde zusätzlich telefonisch kontaktiert; Zusage für Antwort bis Ende März, bislang ohne Reaktion.

Beschluss 2026-KI-008: Wenn bis 30.04.2026 keine vollständige Antwort: Überprüfung alternativer Anbieter bis 30.06.2026 (Petersen). Vertragsergänzung (Incident SLA, EU-AI-Act-Klausel) soll bis 30.04.2026 als Änderungsvereinbarung versandt werden.

TOP 8 — Sonstiges

Roosendaal informiert: Der nächste Quartalsbericht für den Aufsichtsrat ist für die Sitzung am 15. Mai 2026 vorzubereiten. Kühnhausen übernimmt Koordination.

Nächste KI-Komitee-Sitzung: **20. Juni 2026**, 09:00 Uhr, Sitzungszimmer Energiehalle.

*Protokoll erstellt: Claudia Berger-Hentschel, 17.03.2026. Genehmigt: Dr. F. Roosendaal, 20.03.2026.
Aktenzeichen: TI-KI-2026-014.*

Datei: 11-betriebsratsvereinbarung-entwurf.md

Betriebsvereinbarung KI-Systeme — Entwurf

Aktenzeichen: TI-KI-2026-009 (Anlage)

Dokumentversion: 0.5 (Verhandlungsstand 08. April 2026)

Zwischen: Thalheim Industries SE (vertreten durch CCO Annegret Kühnhausen) und dem Betriebsrat der Thalheim Industries SE (vertreten durch Vorsitzenden Norbert Schäpers)

Status: Entwurf; noch nicht unterzeichnet; Verhandlungen laufen

Präambel

Die Thalheim Industries SE setzt im Rahmen ihrer Geschäftstätigkeit KI-gestützte Systeme ein, darunter Hochrisiko-KI-Systeme nach Anhang III der Verordnung (EU) 2024/1689 (KI-Verordnung). Der Betriebsrat macht sein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG (<https://dejure.org/gesetze/BetrVG/87.html>) geltend, da KI-Systeme technische Einrichtungen im Sinne dieser Vorschrift darstellen, die zur Überwachung des Verhaltens oder der Leistung der Arbeitnehmerinnen und Arbeitnehmer bestimmt oder geeignet sind.

Arbeitgeber und Betriebsrat sind sich einig, dass der Einsatz von KI-Systemen transparent, fair und unter Wahrung der Persönlichkeitsrechte der Beschäftigten erfolgen muss. Diese Betriebsvereinbarung regelt die Einführung, den Betrieb und die Überwachung von KI-Systemen, die auf Beschäftigte oder ihre Daten einwirken.

§ 1 Geltungsbereich

Diese Betriebsvereinbarung gilt für alle KI-Systeme der Thalheim Industries SE, die:

1. Beschäftigtendaten verarbeiten oder auswerten,
2. Entscheidungen über Beschäftigte (Einstellung, Beförderung, Leistungsbewertung) unterstützen oder treffen,
3. Verhaltens- oder Leistungsdaten von Beschäftigten analysieren.

Ausdrücklich erfasst: RecruitAI (Recruiting-Screening), CreditVision Score (soweit Beschäftigte betroffen sind), Analyse-Tools im HR-Bereich.

Ausdrücklich nicht erfasst: PredictMaint (keine Beschäftigtendaten), ServiceBot (keine Beschäftigtendaten), CodeAssist (soweit nur für Entwickler-Support).

§ 2 Informationspflichten des Arbeitgebers

§ 2 Abs. 1: Der Arbeitgeber informiert den Betriebsrat vor der Einführung, wesentlichen Änderung oder dem Einsatz neuer KI-Systeme im Sinne von § 1 mindestens sechs Wochen vor dem geplanten Einsatz.

§ 2 Abs. 2: Die Unterrichtung umfasst:

- Zweck und Funktionsweise des KI-Systems in verständlicher Sprache;
- Beschreibung der verarbeiteten Datenkategorien und Betroffenenengruppen;
- Risikoklassifikation nach KI-VO;
- Ergebnis der Datenschutz-Folgenabschätzung (sofern durchgeführt);
- Informationen über den Anbieter (Vendor) und bestehende AVV;
- Ergebnis etwaiger Bias-Tests.

§ 2 Abs. 3: Der Betriebsrat kann auf Kosten des Arbeitgebers bis zu zwei externe Sachverständige für KI-Systeme nach § 80 Abs. 3 BetrVG hinzuziehen. [*Streitpunkt: Arbeitgeber prüft Kostengrenze noch.*]

§ 3 Zustimmungsvorbehalt

§ 3 Abs. 1: Die Inbetriebnahme von KI-Systemen nach § 1 bedarf der Zustimmung des Betriebsrats.

§ 3 Abs. 2: Der Betriebsrat kann die Zustimmung verweigern, wenn:

- die nach § 2 erforderlichen Informationen nicht vollständig vorliegen;
- Bias-Tests mit nicht tolerierbaren Diskriminierungsrisiken abgeschlossen wurden;
- eine erforderliche DPIA nicht vorliegt oder wesentliche Risiken nicht gemindert wurden;
- die Anforderungen dieser Betriebsvereinbarung nicht erfüllt sind.

§ 3 Abs. 3: Verweigert der Betriebsrat die Zustimmung, teilt er dies mit Begründung innerhalb von zwei Wochen nach Unterrichtung mit. Arbeitgeber und Betriebsrat suchen dann gemeinsam eine Lösung. Scheitert die Einigung, ist die Einigungsstelle nach § 76 BetrVG anzurufen.

§ 4 Transparenz und Erklärungsrecht

§ 4 Abs. 1: Beschäftigte, über die ein KI-System Empfehlungen oder Entscheidungen trifft, werden vorab in verständlicher Sprache über den Einsatz des Systems informiert.

§ 4 Abs. 2: Beschäftigte haben das Recht, auf Antrag eine Erklärung der Entscheidungsgrundlage zu erhalten (Art. 22 DSGVO; <https://dejure.org/gesetze/DSGVO/22.html>). Diese Erklärung muss in einfacher

Sprache die wesentlichen Parameter des Scorings beschreiben.

§ 4 Abs. 3: Automatische Entscheidungen ohne menschliche Überprüfung (voll automatisierte Ablehnungen) sind verboten.

§ 5 Menschliche Aufsicht

§ 5 Abs. 1: Bei allen KI-Systemen nach § 1 entscheidet grundsätzlich ein Mensch. Das KI-System ist Entscheidungsunterstützungswerkzeug, kein Entscheidungsträger.

§ 5 Abs. 2: Für RecruitAI gilt: Die abschließende Einstellungs- oder Ablehnungsentscheidung liegt beim zuständigen HR-Business-Partner. Abweichungen vom KI-Ranking sind zu dokumentieren.

§ 6 Bias-Monitoring und regelmäßige Überprüfung

§ 6 Abs. 1: Der Arbeitgeber führt jährlich Bias-Tests für alle KI-Systeme nach § 1 durch und legt die Ergebnisse dem Betriebsrat vor.

§ 6 Abs. 2: Werden Bias-Probleme festgestellt, ist das System sofort anzupassen oder vorübergehend außer Betrieb zu nehmen.

§ 6 Abs. 3: Der Betriebsrat erhält Zugang zu aggregierten Statistiken (Einstellungsquoten, Score-Verteilungen nach Geschlecht, Alter, Nationalität) — keine Einzelpersonendaten.

§ 7 Schulung

§ 7 Abs. 1: Beschäftigte, die KI-Systeme nutzen oder deren Ausgaben berücksichtigen, sind vor Einsatz entsprechend zu schulen (Art. 4 KI-VO, AI Literacy). Die Schulungsnachweise sind dem Betriebsrat auf Anfrage vorzulegen.

§ 7 Abs. 2: Der Betriebsrat und seine Mitglieder erhalten eine eigene Schulung zum Thema KI-Mitbestimmung (Modul G laut AI-Literacy-Curriculum, Aktenstück 05) auf Kosten des Arbeitgebers.

§ 8 Laufzeit und Kündigung

Diese Betriebsvereinbarung gilt auf unbestimmte Zeit. Sie kann von jeder Seite mit einer Frist von sechs Monaten schriftlich gekündigt werden. Bei Kündigung gilt eine Nachwirkung bis zum Abschluss einer neuen Vereinbarung.

Offene Verhandlungspunkte (Stand 08. April 2026)

Punkt	Arbeitgeber-Position	BR-Position	Status
Externe Sachverständige (§ 2 Abs. 3)	Kostenobergrenze 10.000 EUR	Keine Kostenbeschränkung	**Offen**
Reichweite Zustimmungsvorbehalt	Nur Hochrisiko-Systeme	Alle KI nach § 1	**Teileinigung**
Bias-Test-Frequenz	Jährlich	Halbjährlich	**Offen**

Punkt	Arbeitgeber-Position	BR-Position	Status
Score-Einsichtnahme Beschäftigte	Auf Anfrage, schriftlich	Proaktiv vor Entscheidung	**Offen**
Vergütungsregelung BR-Sachverständige	Intern koordinieren	Unabhängige externe	**Offen**

Entwurf v0.5, Verhandlungsstand 08.04.2026. Nicht unterzeichnet. Aktenzeichen: TI-KI-2026-009.

Datei: 12-aufsichtsrat-bericht.md

Aufsichtsratsbericht — KI-Governance Q1 2026

Aktenzeichen: TI-KI-2026-007 (Anlage Aufsichtsrat)

Datum: 15. Mai 2026 (Aufsichtsratssitzung)

Vorgelegt durch: Annegret Kühnhausen, CCO; Dr. Falk Roosendaal, KI-Komitee

Verteilung: Aufsichtsrat Thalheim Industries SE (vertraulich)

1. Zusammenfassung (Executive Summary)

Das KI-Governance-Programm TI-KI-2026 befindet sich in der kritischen Phase 2 (Konformitätsherstellung). Der Vorstand hat im Oktober 2025 das Programm initiiert; die Phase 1 (Inventarisierung) ist abgeschlossen. Der Aufsichtsrat wird gemäß § 90 AktG quartalsweise informiert.

Kritische Feststellungen für den Aufsichtsrat:

- RecruitAI — Bias-Tests fehlen:** Der externe Auditor hat festgestellt, dass der Vendor Synaptec keine Bias-Tests nach Art. 9 Abs. 7 KI-VO dokumentiert hat. Die Frist 02.08.2026 ist in Gefahr. Ein unabhängiges Bias-Testing wurde beauftragt.
- BaFin-Anfrage CreditVision Score:** Die BaFin hat eine förmliche Anfrage (GZ BJ 24-K 7102-2026/0012) gestellt. Antwortfrist 15.05.2026. Thalheim ist im Zusammenspiel mit Kanzlei Borchmann auf die Beantwortung vorbereitet. Haftungsrisiko nach § 93 AktG ist zu beachten.
- Betriebsvereinbarung KI:** Verhandlungen mit dem Betriebsrat laufen seit Januar 2026. Einigung noch nicht erzielt. Kein genehmigter Rollout ohne BV.
- Schulungsrückstand:** 62 % der Mitarbeitenden haben die Pflichtschulung nach Art. 4 KI-VO noch nicht abgeschlossen. Maßnahmenpaket wurde verabschiedet.
- Schatten-KI Marketing:** Nicht genehmigtes KI-Tool identifiziert und abgeschaltet. Aufarbeitung läuft.

2. Programm-Status TI-KI-2026

Meilenstein	Geplant	Status	Bemerkung
Phase 1: KI-Inventarisierung	Dez. 2025	Abgeschlossen ✓	23 Systeme erfasst
Risikoklassifikation	Jan. 2026	Abgeschlossen ✓	2 Hochrisiko identifiziert

Meilenstein	Geplant	Status	Bemerkung
Konformitätsprüfung RecruitAI	Jul. 2026	In Bearbeitung ■	Bias-Test-Mangel
Konformitätsprüfung CreditVision	Jul. 2026	In Bearbeitung ■	BaFin-Anfrage
DPIA RecruitAI	Jun. 2026	In Bearbeitung ■	LfDI BW-Frist
Betriebsvereinbarung KI	Apr. 2026	Verzögert ■	BR-Blockade
AI Literacy (alle Mitarbeitenden)	Okt. 2026	In Bearbeitung (38 %) ■	Rückstand
AI Literacy (HR, Finanzierung)	Mai 2026	In Bearbeitung (36–40 %) ■	Priorisiert
Governance-Leitlinie final	Apr. 2026	In Freigabe ■	Vorstand ausstehend

3. Haftungsrisiken für Vorstand und Aufsichtsrat

3.1 Vorstandshaftung (§ 93 AktG): Gemäß § 93 Abs. 1 AktG (<https://dejure.org/gesetze/AktG/93.html>) haben die Vorstandsmitglieder die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Die pflichtwidrige Nichtimplementierung der KI-VO-Anforderungen kann zu persönlicher Haftung führen. Der Vorstand hat durch Beschluss VS-2025-087 seine Sorgfaltspflicht dokumentiert; die konsequente Programmumsetzung ist unverzichtbar.

3.2 Bußgeldrisiken (KI-VO):

- Verstoß gegen Verbote (Art. 5 KI-VO): bis zu 35 Mio. EUR oder 7 % Jahresumsatz
- Verstoß gegen Hochrisiko-Pflichten (Art. 9–17 KI-VO): bis zu 15 Mio. EUR oder 3 % Jahresumsatz
- Falsche Angaben gegenüber Behörden: bis zu 7,5 Mio. EUR oder 1 % Jahresumsatz

Bei einem Jahresumsatz von rd. 3,2 Mrd. EUR sind die relevanten Obergrenzen:

- Ebene 1 (Art. 5): rd. 224 Mio. EUR (7 % von 3,2 Mrd.)
- Ebene 2 (Hochrisiko): rd. 96 Mio. EUR (3 % von 3,2 Mrd.)

3.3 Aufsichtsratspflichten: Der Aufsichtsrat hat nach § 111 AktG die Geschäftsführung zu überwachen. Der Aufsichtsrat nimmt die vorliegenden Berichte zur Kenntnis und empfiehlt dem Vorstand, dem Programm TI-KI-2026 höchste Priorität einzuräumen.

4. Finanzieller Programmfortschritt

Position	Budget gesamt	Verbraucht (Q1 2026)	Prognose Jahresende
Externe Rechtsberatung (Borchmann)	280.000 EUR	68.000 EUR	220.000 EUR
Externer Auditor (Hagedorn)	190.000 EUR	47.000 EUR	160.000 EUR

Position	Budget gesamt	Verbraucht (Q1 2026)	Prognose Jahresende
Bias-Testing unabhängig (neu)	80.000 EUR	0 EUR	75.000 EUR
AI Literacy Schulungsplattform	95.000 EUR	38.000 EUR	85.000 EUR
Interne Personalaufwände	650.000 EUR	162.000 EUR	600.000 EUR
Technologie-Anpassungen	155.000 EUR	22.000 EUR	140.000 EUR
Gesamt	**1.450.000 EUR**	**337.000 EUR**	**1.280.000 EUR**

Budgetprognose: Programm liegt leicht unter Budget. Kein Nachtragsantrag erforderlich.

5. Empfehlung an den Aufsichtsrat

Der Aufsichtsrat wird gebeten:

1. Den vorliegenden Bericht zur Kenntnis zu nehmen.
2. Den Vorstand zu ermächtigen, im Falle einer Nicht-Einigung mit dem Betriebsrat die Einigungsstelle nach § 76 BetrVG anzurufen.
3. Den Vorstand zu beauftragen, in der nächsten Sitzung (August 2026) über den Abschluss der Konformitätsprüfung RecruitAI zu berichten.

Aktenzeichen: TI-KI-2026-007. Vorgelegt: A. Kühnhausen, Dr. F. Roosendaal. Aufsichtsratssitzung 15. Mai 2026.

Datei: 13-konformitaetspruefung-hr-system.md

Konformitätsprüfung RecruitAI — Auditbericht (Zwischenbericht)

Aktenzeichen: TI-KI-2026-012

Prüfender: WPG Hagedorn & Partner, Frankfurt am Main (Prüfungsleitung: Dr. Miriam Hagedorn)

Auftraggeber: Thalheim Industries SE, CCO Annegret Kühnhausen

Prüfungszeitraum: 15. Januar 2026 – laufend (Abschlussbericht geplant: 31. Juli 2026)

Berichtsdatum: 28. Februar 2026

Berichtstyp: Zwischenbericht

1. Auftrag und Prüfungsumfang

Hagedorn & Partner wurde durch Thalheim Industries SE mandatiert, die Konformitätsbewertung für das Hochrisiko-KI-System **RecruitAI** (Vendor: Synaptec Analytics GmbH) nach Art. 43 Abs. 2 KI-VO zu

begleiten. RecruitAI fällt unter Anhang III Nr. 4 lit. a KI-VO (Personalauswahl/-priorisierung) und ist damit als Hochrisiko-System eingestuft.

Prüfungsgrundlage:

- Art. 9–17 KI-VO (Hochrisiko-Pflichten)
- Art. 43 KI-VO (Konformitätsbewertungsverfahren)
- ISO/IEC 42001 (KI-Managementsystem, informativ)
- NIST AI RMF (informativ)
- Interne Vorgaben Thalheim Industries SE (KI-Governance-Leitlinie v2.1)

Prüfungsumfang:

1. Risikomanagementsystem (Art. 9)
2. Daten-Governance (Art. 10)
3. Technische Dokumentation (Art. 11)
4. Protokollierung (Art. 12)
5. Transparenz / Gebrauchsanweisung (Art. 13)
6. Menschliche Aufsicht (Art. 14)
7. Genauigkeit, Robustheit, Cybersicherheit (Art. 15)
8. Qualitätsmanagementsystem (Art. 17)

2. Prüfungsergebnisse im Überblick

Prüfbereich	Rechtsgrundlage	Ergebnis	Kritikalität
Risikomanagementsystem	Art. 9 KI-VO	Vorhanden; Aktualisierung erforderlich	Mittel
Daten-Governance	Art. 10 KI-VO	Teilweise dokumentiert	Mittel
Bias-Tests	**Art. 9 Abs. 7 KI-VO**	**Fehlen vollständig**	**Kritisch**
Technische Dokumentation	Art. 11 KI-VO	Teilweise (Vendor); Nachforderung läuft	Hoch
Protokollierung	Art. 12 KI-VO	Implementiert; Protokolltiefe prüfen	Niedrig
Gebrauchsanweisung	Art. 13 KI-VO	Vorhanden (DE); ausreichend	Niedrig
Menschliche Aufsicht	Art. 14 KI-VO	Konzept vorhanden; SOP fehlt	Mittel
Override-Mechanismus	Art. 14 Abs. 4 KI-VO	Technisch möglich; SOP fehlt	Mittel
Automatische Ablehnung	Art. 14 / Art. 22 DSGVO	Ohne HR-Aktiv-Bestätigung möglich	**Kritisch**

Prüfbereich	Rechtsgrundlage	Ergebnis	Kritikalität
Genauigkeit / Robustheit	Art. 15 KI-VO	Herstellerangaben; unabhängige Prüfung fehlt	Hoch
Cybersicherheit	Art. 15 KI-VO	Pentest Synaptec-Server ausstehend	Hoch
QMS	Art. 17 KI-VO	ISO 9001 Thalheim; Synaptec ISO 27001	Ausreichend

3. Kritische Feststellungen (Detail)

Feststellung F-001 — Fehlende Bias-Tests (KRITISCH)

Sachverhalt: Die Hagedorn-Prüfung hat ergeben, dass Synaptec Analytics GmbH für das RecruitAI-Modell keine dokumentierten Tests zur Erkennung und Minimierung verzerrter Ausgaben (Bias) nach Art. 9 Abs. 7 KI-VO vorgelegt hat. Synaptec hat auf Anfrage lediglich ein Whitepaper aus dem Jahr 2022 vorgelegt, das allgemeine Fairness-Prinzipien beschreibt, aber keine aktuellen, modellspezifischen Testergebnisse enthält.

Rechtliche Bewertung: Art. 9 Abs. 7 KI-VO verpflichtet Anbieter von Hochrisiko-KI-Systemen, diese auf Bias (Verzerrungen) zu testen, die zu einem in Art. 5 Abs. 1 lit. b GrCh verbotenen Ergebnis führen könnten, namentlich diskriminierende Ergebnisse bei Entscheidungen in Bereichen wie Beschäftigung. Ohne nachweisliche Bias-Tests kann die Konformitätsbewertung nicht mit positivem Ergebnis abgeschlossen werden.

Risikobewertung: KRITISCH. Ohne positive Bias-Test-Ergebnisse:

- Kann die Konformitätserklärung nicht ausgestellt werden (Art. 48 KI-VO).
- Darf das System nach dem 02.08.2026 nicht weiterbetrieben werden.
- Besteht ein erhebliches Diskriminierungsrisiko gegenüber Bewerbern.

Empfehlung: Parallel zu Synaptec sind unabhängige Bias-Tests durch einen spezialisierten Dienstleister zu beauftragen. Dringlichkeit: SOFORT.

Feststellung F-002 — Automatische Ablehnung ohne HR-Bestätigung (KRITISCH)

Sachverhalt: Technische Analyse der Systemlogs zeigt, dass zwischen September 2024 und Februar 2026 in 143 Fällen Bewerberinnen und Bewerber automatisch abgelehnt wurden (Score unter 40), ohne dass eine HR-Mitarbeiterin oder ein HR-Mitarbeiter aktiv eine Ablehnung bestätigt hat. Stattdessen wurde eine automatisierte Ablehnungs-E-Mail durch das System versendet.

Rechtliche Bewertung: Dies stellt einen Verstoß gegen Art. 14 KI-VO (menschliche Aufsicht) und möglicherweise gegen Art. 22 DSGVO (<https://dejure.org/gesetze/DSGVO/22.html>) dar. Art. 22 DSGVO gibt betroffenen Personen das Recht, nicht einer ausschließlich automatisierten Entscheidung unterworfen zu werden, die rechtliche oder ähnlich erhebliche Wirkung entfaltet. Eine Ablehnung einer Bewerbung hat ähnlich erhebliche Wirkung.

Risikobewertung: KRITISCH. Mögliche Haftung gegenüber betroffenen Bewerbern. Meldepflicht nach Art. 35 DSGVO (DPIA) für dieses Verarbeitungsmerkmal. Empfehlung zur Überprüfung der 143 Fälle durch DSB.

Empfehlung: Sofortige technische Sperre der automatischen Ablehnung; aktiver HR-Override als Pflichtschritt.

Feststellung F-003 — Unvollständige technische Dokumentation (HOCH)

Synaptec hat die technische Dokumentation nach Art. 11 i.V.m. Anhang IV KI-VO nur teilweise vorgelegt. Fehlende Abschnitte: Modellarchitektur, Trainingsverfahren, verwendete Datensätze (Herkunft, Umfang, Preprocessing). Nachforderung ist gestellt; Frist 30.04.2026.

4. Positiv bewertete Aspekte

- Protokollierung (Art. 12): Aktiviert und ausreichend tief für Nachvollziehbarkeit.
- Gebrauchsanweisung (Art. 13): In verständlichem Deutsch vorhanden.
- AVV mit Synaptec: Vorhanden und DSGVO-konform.
- IT-Sicherheit Thalheim-Seite: ISO 27001 zertifiziert (gültig bis 06/2027).

5. Weiteres Vorgehen

Maßnahme	Verantwortlich	Frist
Unabhängige Bias-Tests beauftragen (F-001)	CCO / CDO	31.03.2026 ✓ (Beschluss KI-Komitee)
Technische Sperre automatische Ablehnung (F-002)	IT / Synaptec	30.04.2026
Überprüfung 143 Betroffene (F-002)	DSB Dr. Eichenmüller	31.05.2026
Nachforderung Technikdokumentation (F-003)	CIO / Synaptec	30.04.2026
SOP menschliche Aufsicht erstellen	HR	30.04.2026
Pentest Synaptec-Server	IT-Security	31.05.2026
Abschluss Konformitätsprüfung	Hagedorn & Partner	31.07.2026

Zwischenbericht, Aktenzeichen TI-KI-2026-012. WPG Hagedorn & Partner, Frankfurt. Prüfungsleitung Dr. M. Hagedorn. 28.02.2026.

Datei: 14-konformitaetspruefung-kreditscoring.md

Konformitätsprüfung CreditVision Score — Vorbereitende Analyse

Aktenzeichen: TI-KI-2026-015

Dokumentversion: 0.9 (Vorab-Analyse, Audit geplant Mai 2026)

Erstellungsdatum: 25. März 2026

Verfasser: Annegret Kühnhausen (CCO); Rolf Haselmann (Leiter Kundenfinanzierung)

Externe Begleitung: Kanzlei Borchmann Compliance

1. Gegenstand und Ausgangslage

Das Kreditscoring-Modul **CreditVision Score** (Vendor: CreditVision AG, Frankfurt am Main) ist als Hochrisiko-KI-System nach Art. 6 Abs. 2 i.V.m. Anhang III Nr. 5 lit. b KI-VO (<https://dejure.org/gesetze/KIVO/6.html>) klassifiziert. Es berechnet Bonitätsscores für Privat- und Gewerbekunden der Thalheim-Kundenfinanzierungseinheit und fließt in Kreditentscheidungen bei Investitionsgütern und Energieanlagen-Finanzierungen ein.

Die offene BaFin-Anfrage (GZ BJ 24-K 7102-2026/0012, eingegangen 10.03.2026, Antwortfrist 15.05.2026) hat die Konformitätsprüfung zu einem vorrangigen Compliance-Thema gemacht. Die vollständige interne Konformitätsbewertung durch Hagedorn & Partner ist für Mai/Juni 2026 geplant. Das vorliegende Dokument bereitet die Prüfung vor.

2. System-Steckbrief

Merkmal	Inhalt
System	CreditVision Score v4.2
Vendor	CreditVision AG, Mainzer Landstraße 220, 60326 Frankfurt
Vertrag	CV-ENT-2023-TI-0441 (seit 01.04.2023)
Einsatzbereich	Kundenfinanzierung Thalheim Industries SE
Entscheidungsgewicht	Score fließt zu 60 % in Kreditentscheidung ein; 40 % Sachbearbeiter-Urteil
Kreditvolumen p.a.	ca. 340 Mio. EUR (Neuabschlüsse)
Betroffene Personen	Ca. 1.200 Neukunden p.a. (natürliche Personen und Unternehmer)
Datenbasis	Eigenangaben Kunden, Schufa-Score, Kontoauszüge (optionaler PSD2-Zugang), Branchendaten

3. Prüfung Art. 22 DSGVO

Sachverhalt: CreditVision Score unterstützt Kreditentscheidungen, die erhebliche Rechtsfolgen für Kunden haben (Kreditbewilligung oder -ablehnung). Dies fällt unter Art. 22 Abs. 1 DSGVO (<https://dejure.org/gesetze/DSGVO/22.html>), wenn die Entscheidung ausschließlich oder überwiegend auf automatisierter Verarbeitung beruht.

Analyse:

- Bei einem Score-Gewicht von 60 % liegt noch keine „ausschließlich automatisierte“ Entscheidung vor, wenn der Sachbearbeiter aktiv entscheidet.
- Kritisch: In der Praxis folgen Sachbearbeiter dem Score in 94 % der Fälle, was de facto einer automatisierten Entscheidung nahekommt (vgl. EuGH, Urteil vom 07.12.2023, Rs. C-634/21, „SCHUFA Holding AG“ — obiter dicta zur funktionalen Automationsqualität).
- Empfehlung: Sachbearbeiterprozess stärken; aktives Dokumentationserfordernis bei Abweichungen nach oben und unten.

Maßnahmen Art. 22 DSGVO:

- Datenschutzhinweis überarbeiten: Kunden über KreditScoring informieren (Art. 13 DSGVO).
- Erklärungsrecht dokumentieren: Kunden haben Recht auf Erläuterung der Score-Faktoren.
- Widerspruchsrecht verankern: Kunden können menschliche Überprüfung verlangen.

4. Vorprüfung der Hochrisiko-Pflichten

Pflicht	Rechtsgrundlage	Vorabeeschätzung	Handlungsbedarf
Risikomanagementsystem	Art. 9 KI-VO	Vorhanden (CreditVision-intern)	Thalheim-spezifische Ergänzung
Bias-Tests	Art. 9 Abs. 7 KI-VO	Unklar — CreditVision keine Aussage	**Nachforderung dringend**
Daten-Governance	Art. 10 KI-VO	Teilweise dokumentiert	Herkunft Schufa-Daten klären
Technische Dokumentation	Art. 11 KI-VO	Teilweise geliefert	Nachforderung läuft
Protokollierung	Art. 12 KI-VO	Log-Daten vorhanden	Aufbewahrungsfrist prüfen
Gebrauchsanweisung	Art. 13 KI-VO	Vorhanden (DE, EN)	Ausreichend
Menschliche Aufsicht	Art. 14 KI-VO	Prozessual verankert	Dokumentationspraxis verbessern
Genauigkeit / Robustheit	Art. 15 KI-VO	Keine unabhängige Prüfung	Unabhängiges Testing planen
Cybersicherheit	Art. 15 KI-VO	ISO 27001 CreditVision AG	Zertifikat anfordern

5. Inhalt der BaFin-Stellungnahme (Entwurf)

Für BaFin GZ BJ 24-K 7102-2026/0012, Antwortfrist 15.05.2026:

Zu Frage 1 — Art. 22 DSGVO: Thalheim erklärt, dass CreditVision Score Entscheidungsunterstützungs-, kein Entscheidungssystem ist. Die abschließende Kreditentscheidung trifft ein qualifizierter Sachbearbeiter. Die Informationspflichten nach Art. 13 DSGVO werden seit [Datum] durch den aktualisierten Datenschutzhinweis erfüllt. Das Widerspruchsrecht nach Art. 22 Abs. 3 DSGVO ist im Kundenprozess verankert.

Zu Frage 2 — Art. 43 Abs. 2 KI-VO: Die vollständige interne Konformitätsbewertung für CreditVision Score ist für Mai/Juni 2026 geplant und wird von WPG Hagedorn & Partner begleitet. Der Abschlussbericht wird der BaFin nach Fertigstellung (geplant 31.07.2026) übermittelt. Thalheim verpflichtet sich, bis dahin den Status monatlich zu berichten.

6. Risikobewertung Gesamtsystem

Risiko	Bewertung	Maßnahme
Diskriminierung in Kreditentscheidungen	Mittel	Bias-Tests CreditVision beauftragen
Art. 22 DSGVO-Verstoß	Mittel	Dokumentationsprozess stärken
Unvollständige Vendor-Dokumentation	Hoch	Nachforderung, Vertragsstrafe prüfen
BaFin-Sanktion	Niedrig (mit Stellungnahme)	Fristgerechte, vollständige Antwort
Reputationsrisiko	Niedrig bis mittel	Proaktive Kommunikation an BaFin

Aktenzeichen: TI-KI-2026-015. Verfasser: A. Kühnhausen, R. Haselmann. Stand: März 2026.

Datei: 15-stellungnahme-datenschutzbehoerde.md

Stellungnahme gegenüber dem LfDI Baden-Württemberg

Aktenzeichen Thalheim: TI-KI-2026-012

Behördliches AZ: LfDI BW AZ 1-1085.51/2026/045

Datum: 28. April 2026

An: Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Lautenschlagerstraße 20, 70173 Stuttgart

Von: Dr. Carla Eichenmüller, Datenschutzbeauftragte Thalheim Industries SE

Kanzlei: Kanzlei Borchmann Compliance, Frankfurt am Main (Mitzeichnung)

Betreff: Ihre Anforderung vom 02. März 2026 — DPIA RecruitAI / AZ 1-1085.51/2026/045

Sehr geehrter Herr Landesbeauftragter Dr. Brückner,

wir danken für Ihr Schreiben vom 02.03.2026, mit dem Sie die Thalheim Industries SE zur Vorlage einer vollständigen Datenschutz-Folgenabschätzung (DPIA) nach Art. 35 DSGVO für den Einsatz des KI-Systems RecruitAI aufgefordert haben.

Wir nehmen Ihre Anforderung sehr ernst und haben unverzüglich Maßnahmen eingeleitet. Im Folgenden stellen wir den aktuellen Stand dar und berichten über die ergriffenen Maßnahmen.

1. Anerkennung der DPIA-Pflicht

Thalheim Industries SE erkennt an, dass der Einsatz von RecruitAI (Synaptec Analytics GmbH) zur automatisierten Bewertung und Priorisierung von Bewerbungsunterlagen eine DPIA-pflichtige Verarbeitungstätigkeit nach Art. 35 Abs. 1 und Abs. 3 lit. a DSGVO (<https://dejure.org/gesetze/DSGVO/35.html>) darstellt, da:

- eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (Bewerberinnen und Bewerber) auf Grundlage automatisierter Verarbeitung einschließlich Profiling vorliegt und
- diese Bewertung Entscheidungen nach sich zieht, die für die betroffenen Personen rechtliche oder ähnlich erhebliche Wirkung entfalten (Einstellungsentscheidung).

Die DPIA-Pflicht ist durch die Aufnahme derartiger Systeme in die LfDI-BW-Positivliste (Stand Oktober 2024) bekräftigt.

2. Stand der DPIA-Erarbeitung

Die DPIA befindet sich derzeit in der Entwurfsphase (Version 0.8, Stand März 2026). Die Fertigstellung und Vorlage an Ihre Behörde ist bis zum 30. Juni 2026 geplant. Folgende Schritte sind abgeschlossen:

- Systembeschreibung und Verarbeitungsdokumentation: abgeschlossen (Aktenstück 07)
- Identifikation der Datenkategorien und Betroffengruppen: abgeschlossen
- Risikoidentifikation: abgeschlossen (Risikomatrix liegt vor)
- Einbindung der Datenschutzbeauftragten nach Art. 35 Abs. 2 DSGVO: durchgehend gegeben

Noch ausstehend:

- Bias-Test-Ergebnisse des Vendors Synaptec (Frist 30.05.2026); parallel laufen unabhängige Tests
- Vollständige Risikomaßnahmen-Dokumentation (nach Vorlage Bias-Tests)
- Konsultationsentscheidung nach Art. 36 DSGVO (sofern verbleibende Risiken nicht mitigierbar)

3. Sofortmaßnahmen aufgrund des Audit-Zwischenberichts

Im Rahmen der parallel laufenden Konformitätsprüfung nach KI-VO wurden folgende Sofortmaßnahmen ergriffen:

Maßnahme 1: Die automatische Ablehnung von Bewerberinnen und Bewerbern durch RecruitAI ohne aktive menschliche Bestätigung wurde technisch gesperrt (Umsetzung bis 30.04.2026). Jede Ablehnung erfordert nun eine aktive Bestätigung durch den zuständigen HR-Business-Partner.

Maßnahme 2: Der Datenschutzhinweis im Karriereportal der Thalheim Industries SE wurde am 25.03.2026 aktualisiert und informiert Bewerberinnen und Bewerber nunmehr ausdrücklich über den Einsatz eines KI-gestützten Bewerbungsscreening-Systems sowie ihre Rechte nach Art. 13 und Art. 22 DSGVO.

Maßnahme 3: Für den Zeitraum September 2024 bis Februar 2026 wird geprüft, ob Bewerberinnen und Bewerber, die vollautomatisch abgelehnt wurden (143 Fälle), nachträglich zu informieren sind (Art. 34 DSGVO). Ergebnis der Prüfung bis 31.05.2026.

4. Zeitplanung

Meilenstein	Termin
Technische Sperre automatische Ablehnung	30.04.2026
Bias-Test-Ergebnisse Synaptec	30.05.2026
Unabhängige Bias-Test-Ergebnisse	30.06.2026
Fertigstellung DPIA	30.06.2026
Übermittlung DPIA an LfDI BW	30.06.2026
Entscheidung über Konsultation nach Art. 36 DSGVO	Nach DPIA-Fertigstellung

5. Bitte um Fristverlängerung / Zwischenstatus

Thalheim Industries SE bittet das LfDI BW um Bestätigung, dass die Einreichung der vollständigen DPIA zum 30. Juni 2026 akzeptiert wird. Wir sichern zu, dass wir bis dahin monatliche Zwischenberichte (jeweils zum 15. des Monats) vorlegen werden.

Für Rückfragen stehe ich jederzeit zur Verfügung.

Mit freundlichen Grüßen

Dr. Carla Eichenmüller Datenschutzbeauftragte Thalheim Industries SE August-Bebel-Ring 14, 68163 Mannheim T: +49 621 9340-2201 c.eichenmueller@thalheim-industries.de

Annegret Kühnhausen (CCO, Mitzeichnung)

Dr. Nora Borchmann (Kanzlei Borchmann Compliance, Mitzeichnung)

Aktenzeichen: TI-KI-2026-012. LfDI BW: AZ 1-1085.51/2026/045. Datum: 28.04.2026.

Datei: 16-interner-audit-bericht.md

Interner Revisionsbericht — KI-Compliance (März/April 2026)

Aktenzeichen: TI-KI-2026-016

Dokumentversion: 1.0 (Endfassung)

Datum: 02. Mai 2026

Verfasser: Franz-Josef Brammer, Leiter Konzernrevision Thalheim Industries SE

Verteiler: CEO Dr. Thalheim-Lattermann; CCO Kühnhausen; CIO Dr. Wolfsbacher; CDO Petersen; KI-Komitee

1. Prüfungsauftrag und Methodik

Die Konzernrevision hat im Zeitraum März/April 2026 eine anlassbezogene und routinemäßige KI-Compliance-Prüfung durchgeführt. Anlassbezogener Auslöser war die Entdeckung des nicht genehmigten GenAI-Tools in der Marketingabteilung am 14.03.2026 (sog. Schatten-KI). Die Prüfung wurde auf das gesamte KI-Governance-Programm TI-KI-2026 ausgeweitet.

Prüfungsmethoden:

- Dokumentenanalyse (KI-Inventar, Governance-Dokumentation, Vendor-Verträge)
- Interviews mit verantwortlichen Personen (CIO, CDO, CCO, DSB, HR, Finanzierung, IT-Security)
- Technische Sichtprüfung (Systemzugriffe, Log-Analyse)
- Vergleich mit internen Richtlinien (KI-Governance-Leitlinie v2.1) und externen Anforderungen (KI-VO, DSGVO)

2. Feststellungen

Feststellung R-001 — Schatten-KI Marketingabteilung (KRITISCH)

Sachverhalt: Die Marketingabteilung (Leiter: Dr. Philipp Sonntag) hat seit Juli 2025 (Beginn geschätzt auf Basis erster Log-Daten) ein nicht genehmigtes KI-Tool (Midjourney API-Integration über eigens eingerichteten Server) für Bildgenerierung und Texterstellung eingesetzt. Das Tool wurde außerhalb des zentralen CDO-verwalteten IT-Stack betrieben und war weder im KI-Inventar eingetragen noch durch den KI-Freigabeprozess genehmigt worden.

Volumen: Mindestens 8 Monate Betrieb; ca. 2.400 API-Anfragen (rekonstruiert aus Cloud-Kostenabrechnungen).

Datenrisiko: Prüfung durch DSB Dr. Eichenmüller ergab, dass in 34 von 2.400 Anfragen Nachnamen und Firmennamen von Kunden in Prompts eingegeben wurden. Diese Daten wurden an die Midjourney-Server (USA, keine adequate-level-Entscheidung für diesen Verarbeitungskontext) übermittelt. Potenzielle DSGVO-Verletzung (Art. 44 ff. DSGVO); Meldepflicht an LfDI BW wird geprüft.

Ursachen: (1) Fehlende technische Zugangskontrollen (API-Nutzung nicht geblockt); (2) Unzureichende Sensibilisierung der Führungskräfte (AI-Literacy-Rückstand); (3) Unklare Kommunikation der KI-Governance-Anforderungen.

Empfehlung: Sofortige Überprüfung und Sperrung nicht autorisierter API-Endpunkte. Arbeitsrechtliche Konsequenzen für Dr. Sonntag prüfen (nach Anhörung). Nachträgliche Datenschutzprüfung der 34 Kundendaten-Fälle. Eskalation an LfDI BW ggf. nach Art. 33 DSGVO.

Feststellung R-002 — AI-Literacy-Schulungsrückstand als systemisches Risiko (HOCH)

Sachverhalt: Nur 38 % aller Mitarbeitenden haben Modul A abgeschlossen (Stand März 2026). In Fachbereichen mit Hochrisiko-Systemen (HR: 36 %, Finanzierung: 40 %) besonders kritisch. Der Betriebsrat hat noch keinerlei Schulung erhalten.

Bewertung: Das Vorkommnis mit der Schatten-KI in der Marketingabteilung ist unmittelbar auf den Schulungsrückstand zurückzuführen. Dr. Sonntag und sein Team wussten nicht um die KI-Freigabepflicht. Dies zeigt: der Schulungsrückstand ist kein administratives Problem, sondern ein systemisches Compliance-Risiko.

Empfehlung: Sofortprogramm AI Literacy mit Führungskräftepflicht. Monatliches Reporting an KI-Komitee. Kopplung der Freigabe neuer KI-Tools an Schulungsnachweis des Antragstellers.

Feststellung R-003 — Keine vollständige Vendor-Vertragsrevision nach KI-VO (MITTEL)

Sachverhalt: Die Bestandsverträge mit Synaptec Analytics GmbH und CreditVision AG enthalten keine KI-VO-spezifischen Klauseln (Bias-Test-Pflichten, Meldepflichten bei Incidents, technische Dokumentations-SLA). Der OpenAI-Vertrag enthält ebenfalls keine EU-AI-Act-Klausel.

Bewertung: Thalheim trägt als Betreiber die Verantwortung dafür, dass die Vendor-Systeme die KI-VO-Anforderungen erfüllen. Fehlende vertragliche Absicherung erhöht das Haftungsrisiko.

Empfehlung: Alle Vendor-Verträge bis 30.06.2026 um KI-VO-Klauseln ergänzen (Nachtragsvereinbarung). Dabei insbesondere: Bias-Test-Pflicht, techn. Dokumentations-SLA, Incident-Meldepflicht 24h, Konformitätserklärung-Pflicht vor Inbetriebnahme neuer Modellversionen.

Feststellung R-004 — Fehlende SOP für menschliche Aufsicht RecruitAI (MITTEL)

Sachverhalt: Es gibt keine schriftlich dokumentierte SOP (Standard Operating Procedure) für HR-Business-Partner, wann und wie sie RecruitAI-Empfehlungen überstimmen sollen. Schulungsmaterial ist vorhanden, aber kein verbindliches Protokollierungsverfahren für Override-Entscheidungen.

Empfehlung: SOP bis 30.04.2026 erstellen und in LMS einbinden. Jede Override-Entscheidung in SAP SuccessFactors dokumentieren.

Feststellung R-005 — KI-Inventar unvollständig (NIEDRIG)

Sachverhalt: Das KI-Inventar enthält 23 Systeme. Im Rahmen der Bereichsbefragung im April 2026 wurden weitere 4 Systeme gemeldet, die noch nicht eingetragen waren (darunter 1 weiteres Marketing-Tool, 2 Analyse-Tools im Vertrieb, 1 KI-basierter Outlook-Assistent).

Empfehlung: Inventar-Kampagne wiederholen. Bis 30.06.2026 alle Meldungen verarbeiten und Inventar abschließen.

3. Bewertungsübersicht

Feststellung	Kritikalität	Status (April 2026)	Frist
R-001 Schatten-KI Marketing	Kritisch	Abgeschaltet; Aufarbeitung läuft	31.05.2026
R-002 AI-Literacy-Rückstand	Hoch	Maßnahmenpaket verabschiedet	31.10.2026
R-003 Vendor-Vertrags revision	Mittel	In Vorbereitung	30.06.2026
R-004 SOP menschliche Aufsicht	Mittel	In Erarbeitung	30.04.2026
R-005 KI-Inventar unvollständig	Niedrig	Kampagne geplant	30.06.2026

4. Managementreaktion

CCO Kühnhausen hat den Bericht am 28.04.2026 entgegengenommen und alle Empfehlungen akzeptiert. Die Konzernrevision wird den Umsetzungsstand der Maßnahmen im Rahmen der nächsten Routineprüfung (Q3 2026) nachverfolgen.

Revisionsbericht R-2026-005. Aktenzeichen: TI-KI-2026-016. Leiter Konzernrevision: Franz-Josef Brammer. 02.05.2026.

Datei: 17-eskalation-vorstandsvorsitz.md

Eskalationsvorlage an den Vorstandsvorsitzenden

Aktenzeichen: TI-KI-2026-007

Datum: 15. April 2026

An: Dr. Reinhard Thalheim-Lattermann, CEO

Von: Annegret Kühnhausen, CCO; Dr. Falk Roosendaal, KI-Komitee-Vorsitz

Klassifizierung: VERTRAULICH — NUR FÜR VORSTANDSMITGLIEDER

Betreff: Eskalation — Kumulative Risiken KI-Governance-Programm TI-KI-2026

Sehr geehrter Herr Dr. Thalheim-Lattermann,

wir berichten Ihnen über eine Verdichtung kritischer Risiken im KI-Governance-Programm TI-KI-2026, die eine Entscheidung auf Vorstandsebene erfordern. Drei Stränge entwickeln sich so, dass ohne Ihr persönliches Eingreifen die gesetzliche Frist 02.08.2026 für RecruitAI nicht zu halten ist und erhebliche behördliche und reputationsbezogene Konsequenzen drohen.

1. Situationsbeschreibung

Strang 1: RecruitAI — Doppeltes Risiko (Bias-Tests + automatische Ablehnungen)

Der Auditor Hagedorn & Partner hat am 28.02.2026 festgestellt:

- Synaptec Analytics GmbH hat **keine dokumentierten Bias-Tests** geliefert. Nach 6 Wochen keine Reaktion auf unsere Mahnung vom 05.03.2026.
- In **143 Fällen** wurden Bewerberinnen und Bewerber vollautomatisch abgelehnt — ohne HR-Bestätigung. Dies ist ein potenzieller Verstoß gegen Art. 22 DSGVO und Art. 14 KI-VO.

Was bereits getan wurde: Technische Sperre der automatischen Ablehnung ab 30.04.2026; paralleles Bias-Testing beauftragt; LfDI BW informiert.

Was fehlt: Synaptec liefert nicht. Wenn bis 30.05.2026 keine Bias-Test-Ergebnisse vorliegen, können wir die Konformitätsbewertung bis 31.07.2026 nicht abschließen. In diesem Fall müsste RecruitAI ab 02.08.2026 abgeschaltet werden.

Entscheidungsbedarf: Sollen wir rechtliche Schritte gegen Synaptec wegen Vertragsverletzung einleiten? Und sollen wir parallel ein alternatives Recruiting-System evaluieren? Dies erfordert Ihr Mandat und Budgetfreigabe für externe Rechtsberatung (Schätzung: 50.000 EUR) und System-Evaluation (Schätzung: 120.000 EUR).

Strang 2: Betriebsrat — Keine Einigung in Sicht

Die Betriebsvereinbarungsverhandlungen laufen seit Januar 2026. Trotz drei Gesprächen besteht keine Einigung zu den Kernpunkten (Sachverständige, Bias-Test-Frequenz, Einsichtnahme).

Betriebsratsvorsitzender Schäpers hat in der letzten Sitzung am 08.04.2026 signalisiert, er erwäge einen Antrag auf einstweilige Verfügung, wenn der Rollout ohne BV versucht wird.

Konsequenz: Ohne abgeschlossene BV können RecruitAI und CreditVision Score nach § 87 BetrVG nicht regulär weiterbetrieben werden. Der Betriebsrat hat ein Klagerecht beim Arbeitsgericht.

Entscheidungsbedarf: Ermächtigen Sie die CCO, die Einigungsstelle nach § 76 BetrVG (<https://dejure.org/gesetze/BetrVG/76.html>) anzurufen, wenn bis 15.05.2026 keine Einigung erzielt wird? Das Einigungsstellenverfahren kostet ca. 25.000–60.000 EUR und dauert 3–6 Monate, bietet aber einen geordneten Abschluss.

Strang 3: Schatten-KI Marketing — Mögliche DSGVO-Meldepflicht

Die Konzernrevision hat festgestellt, dass in 34 Fällen Kundendaten in Midjourney-Prompts eingegeben wurden, die an Server in den USA übermittelt wurden. Die Datenschutzbeauftragte Dr. Eichenmüller prüft, ob eine Meldung nach Art. 33 DSGVO an den LfDI BW erforderlich ist.

Konsequenz: Wenn eine Meldepflicht besteht, muss diese innerhalb von 72 Stunden nach Kenntnis des Risikos erfolgen. Die Kenntnis des Datenschutzvorfalls entstand am 20.04.2026; Frist läuft.

Entscheidungsbedarf: Autorisieren Sie Dr. Eichenmüller, die Meldung nach Art. 33 DSGVO zu erstatten, sofern ihre rechtliche Prüfung eine Meldepflicht ergibt — ohne weitere Rückfrage beim Vorstand? Hintergrund: Schnelligkeit ist hier Pflicht.

2. Handlungsoptionen im Überblick

Entscheidung	Option A	Option B	Empfehlung CCO
Synaptec-Eskalation	Rechtliche Schritte + Alternativsystem	Weiter warten	**Option A**
BR-Verhandlung	Einigungsstelle § 76 BetrVG	Verhandlung fortsetzen	**Option A, wenn bis 15.05. keine Einigung**
DSGVO-Meldung	DSB entscheidet autonom	Vorstand entscheidet	**Option A**

3. Finanzieller Bedarf

Position	Betrag	Freigabe erforderlich
Rechtsberatung Synaptec (Vertragsdurchsetzung)	50.000 EUR	Ja
Alternativsystem-Evaluation (parallel)	120.000 EUR	Ja
Einigungsstelle BetrVG (geschätzt)	45.000 EUR	Ja

Position	Betrag	Freigabe erforderlich
Gesamt	**215.000 EUR**	Außerhalb bisherigem Budget

4. Votum der CCO

Ich empfehle, alle drei Entscheidungen so zu treffen, wie unter Option A beschrieben. Das Risiko eines Scheiterns der KI-VO-Konformität bis 02.08.2026 ist aus meiner Sicht erheblicher als der finanzielle Aufwand. Ein Betrieb von RecruitAI ohne Konformitätsnachweis nach dem 02.08.2026 ist rechtlich unzulässig und stellt für den Vorstand eine persönliche Haftung nach § 93 AktG dar.

Bitte teilen Sie uns Ihre Entscheidung bis 22. April 2026 mit.

Mit freundlichen Grüßen

Annegret Kühnhausen, CCO

Dr. Falk Roosendaal, KI-Komitee-Vorsitz

Aktenzeichen: TI-KI-2026-007. Datum: 15.04.2026. VERTRAULICH.

Datei: 18-pressemitteilung-entwurf.md

Pressemitteilung — Entwurf (nicht freigegeben)

Aktenzeichen: TI-KI-2026-007 (Kommunikationsanhang)

Dokumentversion: Entwurf v1.2

Erstellungsdatum: 20. März 2026

Verfasserin: Katharina Voss-Heidemann, Leiterin Unternehmenskommunikation

Abstimmung: Ausstehend — CCO, CEO, Kanzlei Borchmann

Freigabe geplant: nach Abschluss Konformitätsprüfung (Q3 2026)

EMBARGIERT — NUR ZUR INTERNEN ABSTIMMUNG

Pressemitteilung

Mannheim, [Datum nach Freigabe]

Thalheim Industries SE startet umfassendes KI-Governance-Programm — Konformität mit EU-KI-Verordnung bis August 2026

Die Thalheim Industries SE, führendes Unternehmen im deutschen Anlagenbau und in der Energietechnik mit Sitz in Mannheim, gibt den Start ihres konzernweiten KI-Governance-Programms bekannt. Mit dem Programm bereitet sich Thalheim Industries auf die vollständige Konformität mit der Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-VO) vor, die für Hochrisiko-KI-Systeme ab dem 2. August 2026 verbindlich gilt.

„Wir sehen die EU-KI-Verordnung nicht als Bürde, sondern als Chance, das Vertrauen unserer Kunden, Mitarbeiterinnen und Mitarbeiter sowie Geschäftspartner in unsere technologischen Entscheidungen zu stärken“, sagte Dr. Reinhard Thalheim-Lattermann, Vorstandsvorsitzender der Thalheim Industries SE.

„Künstliche Intelligenz ist ein zentraler Baustein unserer digitalen Transformation. Governance ist der Rahmen, der sicherstellt, dass wir diese Technologie verantwortungsvoll einsetzen.“

[*Redaktionelle Anmerkung: Zitat mit CEO noch abzustimmen.*]

KI-Governance als Wettbewerbsvorteil

Thalheim Industries setzt derzeit fünf KI-Systeme in operativem Betrieb ein, darunter KI-gestützte Systeme in den Bereichen Personalauswahl, Kundenfinanzierung, Predictive Maintenance und Software-Entwicklung sowie im Kundenservice. Zwei dieser Systeme — das Recruiting-Screening-Tool und das Kredit scoring-Modul — sind als Hochrisiko-KI-Systeme im Sinne der KI-VO eingestuft und werden einer vollständigen externen Konformitätsprüfung unterzogen.

Dr. Sigrid Wolfsbacher, Chief Information Officer: „Wir haben ein zentrales KI-Inventar aufgebaut und alle eingesetzten Systeme klassifiziert. Das gibt uns die Transparenz, die wir brauchen, um verantwortungsvoll zu handeln.“

KI-Kompetenz für alle Mitarbeiterinnen und Mitarbeiter

Ein Kernbestandteil des Programms ist die konzernweite AI-Literacy-Initiative: Alle 12.000 Mitarbeiterinnen und Mitarbeiter erhalten bis Oktober 2026 eine Schulung zum verantwortungsvollen Umgang mit KI-Systemen — von den Grundlagen bis zur fachbereichsspezifischen Vertiefung für Nutzer von Hochrisiko-Systemen.

Datenschutz als integraler Bestandteil

„Datenschutz und KI-Governance gehen bei uns Hand in Hand“, erklärt Dr. Carla Eichenmüller, Datenschutzbeauftragte der Thalheim Industries SE. „Wo ein KI-System personenbezogene Daten verarbeitet, führen wir eine Datenschutz-Folgenabschätzung durch und setzen klare Grenzen für die automatisierte Entscheidungsunterstützung.“

Mitarbeitervertretung eingebunden

Thalheim Industries verhandelt parallel eine Betriebsvereinbarung zu KI-Systemen mit dem Betriebsrat. [*Redaktionelle Anmerkung: Formulierung abhängig vom Verhandlungsstand zum Freigabezeitpunkt.*]

Über Thalheim Industries SE Die Thalheim Industries SE ist ein führendes deutsches Industrieunternehmen im Bereich Anlagenbau und Energietechnik mit Hauptsitz in Mannheim. Mit rund 12.000 Mitarbeiterinnen und Mitarbeitern und einem Jahresumsatz von ca. 3,2 Milliarden Euro (2025) ist Thalheim Industries in 18 Ländern tätig. Das Unternehmen ist im MDAX gelistet.

Pressekontakt: Katharina Voss-Heidemann Leiterin Unternehmenskommunikation Thalheim Industries SE T: +49 621 9340-3100 presse@thalheim-industries.de

ENTWURF. Nicht zur Veröffentlichung freigegeben. Interne Abstimmung läuft. Aktenzeichen: TI-KI-2026-007.

Datei: 19-q-and-a-kundenanfragen.md

Q&A — Kundenanfragen zum KI-Einsatz bei Thalheim Industries SE

Aktenzeichen: TI-KI-2026-007 (Kommunikationsanhang)

Dokumentversion: 1.1

Erstellungsdatum: 15. April 2026

Verfasserinnen: Katharina Voss-Heidemann (Unternehmenskommunikation); Annegret Kühnhausen (CCO)

Zielgruppe: Vertriebsmitarbeiterinnen und -mitarbeiter, Kundenbetreuer, Pressestelle

Zweck dieses Dokuments

Dieses Q&A-Dokument bereitet häufige Fragen von Kunden, Geschäftspartnern und Medienvertretern zum KI-Einsatz bei Thalheim Industries SE mit genehmigten Antworten vor. Die Antworten sind nicht zur wortwörtlichen Wiedergabe gedacht, sondern als inhaltliche Leitlinie.

Teil A: Allgemeine Fragen

Frage A1: Setzt Thalheim Industries KI-Systeme ein?

Ja. Thalheim Industries setzt derzeit fünf KI-Systeme in verschiedenen Geschäftsbereichen ein: im Bereich Personalauswahl, Kundenfinanzierung, Wartungsplanung für Industrieanlagen, Softwareentwicklung und im Kundenservice-Bereich. Alle Systeme sind klassifiziert und registriert.

Frage A2: Entsprechen die KI-Systeme der EU-KI-Verordnung?

Thalheim Industries nimmt die Anforderungen der Verordnung (EU) 2024/1689 sehr ernst. Das Unternehmen befindet sich in einem aktiven Konformitätsprogramm (TI-KI-2026), das die vollständige Compliance mit den gesetzlichen Fristen anstrebt. Für die zwei als Hochrisiko eingestuften Systeme läuft eine externe Konformitätsprüfung.

Frage A3: Was ist ein Hochrisiko-KI-System?

Die EU-KI-Verordnung stuft KI-Systeme, die in bestimmten sensiblen Bereichen eingesetzt werden, als Hochrisiko ein — darunter Systeme zur Personalauswahl und zur Bewertung der Kreditwürdigkeit. Für diese Systeme gelten strenge Anforderungen: Risikomanagement, Bias-Tests, transparente Dokumentation, menschliche Aufsicht und regelmäßige Prüfungen.

Teil B: Fragen zu Kreditentscheidungen (CreditVision Score)

Frage B1: Entscheidet ein KI-System, ob ich einen Kredit bekomme?

Nein — die abschließende Kreditentscheidung trifft stets ein qualifizierter Kundenbetreuer bei Thalheim Industries. Das KI-Scoring-System berechnet eine Kennzahl, die in die Entscheidungsfindung einfließt, aber keine finale Entscheidung trifft. Der Mensch entscheidet.

Frage B2: Welche Daten werden für das Kredit-Scoring verwendet?

Für die Bonitätsbewertung werden Daten aus Ihrer Selbstauskunft, Angaben zur wirtschaftlichen Situation und — mit Ihrer Einwilligung — Daten im Rahmen des PSD2-Kontodatenzugangs verwendet. Details entnehmen Sie unserer Datenschutzerklärung.

Frage B3: Kann ich eine Erklärung des Scorings verlangen?

Ja. Sie haben nach Art. 22 Abs. 3 DSGVO (<https://dejure.org/gesetze/DSGVO/22.html>) das Recht, die Überprüfung durch einen Mitarbeiter zu verlangen und eine Erklärung zu den wesentlichen Parametern des Scorings zu erhalten. Wenden Sie sich dazu an Ihren Kundenbetreuer oder schreiben Sie an datenschutz@thalheim-industries.de.

Frage B4: Die BaFin hat nach Ihrem Kreditscoring-System gefragt — gibt es Probleme?

Thalheim Industries kooperiert vollständig mit den Aufsichtsbehörden. Der Dialog mit der BaFin läuft im Rahmen der normalen Aufsichtspraxis und dient der Klärung regulatorischer Anforderungen. Wir haben keine Hinweise auf Regelverstöße.

Teil C: Fragen zum Recruiting-Screening (RecruitAI)

Frage C1: Bewertet ein Algorithmus meine Bewerbung bei Thalheim Industries?

Thalheim Industries nutzt ein KI-unterstütztes System, das Bewerbungsunterlagen nach definierten Kriterien auswertet und eine Priorisierungsempfehlung erstellt. Die abschließende Entscheidung, ob ein Bewerber oder eine Bewerberin in die nächste Runde kommt, trifft eine qualifizierte HR-Mitarbeiterin oder ein HR-Mitarbeiter.

Wir informieren Bewerberinnen und Bewerber über den Einsatz dieses Systems in unserer Datenschutzerklärung im Karriereportal.

Frage C2: Diskriminiert das System Bewerber aufgrund von Geschlecht, Herkunft oder Alter?

Thalheim Industries nimmt die Fairness-Anforderungen des KI-Rechts sehr ernst. Wir lassen das System durch externe Fachleute auf Diskriminierungsrisiken testen (sog. Bias-Tests). Die Ergebnisse dieser Tests fließen in die Weiterentwicklung des Systems ein. Bis zum Vorliegen der vollständigen Testergebnisse betreiben wir das System mit verstärkter menschlicher Aufsicht.

Frage C3: Kann ich Auskunft darüber verlangen, welche Daten über mich verarbeitet wurden?

Ja. Sie haben nach Art. 15 DSGVO das Recht auf Auskunft über Ihre gespeicherten Daten und nach Art. 22 DSGVO das Recht, nicht ausschließlich auf Basis automatisierter Entscheidungen beurteilt zu werden. Wenden Sie sich an datenschutz@thalheim-industries.de.

Teil D: Fragen zu Datenschutz und Datensicherheit

Frage D1: Werden meine Daten an KI-Firmen weitergegeben?

Thalheim Industries setzt KI-Systeme von spezialisierten Anbietern ein. Mit allen Anbietern bestehen Auftragsverarbeitungsverträge nach Art. 28 DSGVO, die die Verarbeitung auf den vereinbarten Zweck begrenzen und die Datensicherheit sicherstellen. Datenweitergaben außerhalb des Europäischen Wirtschaftsraums (EWR) erfolgen nur mit geeigneten Schutzmaßnahmen nach Art. 44 ff. DSGVO.

Frage D2: Was ist mit dem Bericht über ein nicht genehmigtes KI-Tool in Ihrer Marketingabteilung?

Thalheim Industries hat intern ein nicht genehmigtes Tool identifiziert, das ein Mitarbeiter ohne entsprechende Freigabe eingesetzt hat. Das Tool wurde sofort abgeschaltet. Wir haben den Vorfall aufgearbeitet und technische und organisatorische Maßnahmen ergriffen, um solche Fälle künftig zu verhindern. Soweit Kundendaten betroffen sind, haben wir die zuständige Datenschutzbehörde informiert.

Aktenzeichen: TI-KI-2026-007. Verfasserinnen: K. Voss-Heidemann, A. Kühnhausen. Version 1.1, April 2026.

Datei: 20-roadmap-konformitaet-2027.md

Konformitäts-Roadmap 2025–2027 — KI-Governance Thalheim Industries SE

Aktenzeichen: TI-KI-2026-007
Dokumentversion: 2.0
Erstellungsdatum: 20. Januar 2026 (aktualisiert März 2026)
Verfasser: Dr. Falk Roosendaal; Annegret Kühnhausen
Freigegeben durch: KI-Komitee, 14.03.2026

1. Überblick

Diese Roadmap zeigt den Weg zur vollständigen Konformität der Thalheim Industries SE mit der Verordnung (EU) 2024/1689 (KI-VO) bis zum 02. August 2027 (finale Anwendungsfrist für alle Hochrisiko-Systeme; bestehende Hochrisiko-Systeme aus Anhang-I-Produkten). Für die primär relevanten Hochrisiko-Systeme RecruitAI und CreditVision Score gilt die Frist 02. August 2026.

Rechtliche Fristen (Art. 113 KI-VO, <https://dejure.org/gesetze/KIVO/113.html>):

Datum	Anwendbare Pflichten
02.02.2025	Art. 5 (Verbote); Art. 50 (Transparenz); Art. 3 (Definitionen)
02.08.2025	Kapitel I (Allg. Bestimmungen); Art. 4 (AI Literacy); Kap. II-IV (Governance)
02.08.2026	Art. 6–51 (Hochrisiko-Pflichten, Konformitätsbewertung, Registrierung)
02.08.2027	Art. 6 für Produkte nach Anhang I (bestehende CE-Produkte)

2. Meilensteinplan

Phase 1: Bestandsaufnahme (Oktober–Dezember 2025) ✓ ABGESCHLOSSEN

Meilenstein	Frist	Status
KI-Inventar: Alle Systeme erfasst	31.12.2025	✓ Abgeschlossen (23 Systeme)
Risikoklassifikation aller Systeme	15.01.2026	✓ Abgeschlossen
Gap-Analyse je System	31.01.2026	✓ Abgeschlossen
KI-Komitee erste Sitzung	15.01.2026	✓ Stattgefunden
Externe Berater mandatiert	15.11.2025	✓ Borchmann, Hagedorn

Phase 2: Konformitätsherstellung (Januar–Juli 2026) — LAUFEND

2A — Rechtliche und Governance-Grundlagen

Meilenstein	Frist	Status (März 2026)
KI-Governance-Leitlinie v2 final + Vorstandsfreigabe	15.04.2026	In Freigabe
Rote Liste (Art. 5) kommuniziert	01.02.2026	✓ Erledigt
ServiceBot: Art. 50-Hinweis implementiert	01.02.2025	✓ Erledigt
Betriebsvereinbarung KI unterzeichnet	30.06.2026	■ Verhandlungen stocken
Vendor-Verträge KI-VO-Klauseln ergänzt	30.06.2026	In Bearbeitung

2B — AI Literacy (Art. 4 KI-VO)

Meilenstein	Frist	Status (März 2026)
Modul A: alle Mitarbeitenden (Ziel 100 %)	31.10.2026	38 % — Kampagne läuft
Modul C: HR-Fachbereich (100 %)	31.05.2026	36 %
Modul D: Finanzierung (100 %)	31.05.2026	40 %
Modul E: IT-Bereich (100 %)	30.06.2026	58 %
Modul F: Compliance (100 %)	30.04.2026	78 %
Modul G: Betriebsrat	31.07.2026	0 %

2C — RecruitAI: Konformitätsprüfung

Meilenstein	Frist	Status (März 2026)
Audit-Start Hagedorn & Partner	15.01.2026	✓ Gestartet
Bias-Test beauftragen (unabhängig)	31.03.2026	✓ Beauftragte (Beschluss KI-Komitee)
Bias-Test-Ergebnisse Synaptec	30.05.2026	■ Offen
Bias-Test-Ergebnisse unabhängig	30.06.2026	In Durchführung
DPIA abgeschlossen + LfDI BW vorlegen	30.06.2026	■ Entwurf v0.8

Meilenstein	Frist	Status (März 2026)
Techn. Dokumentation Synaptec vollst.	30.04.2026	■ Nachforderung
SOP menschliche Aufsicht HR	30.04.2026	In Erarbeitung
Konformitätsbewertung Abschlussbericht	31.07.2026	Geplant
EU-Datenbank-Registrierung RecruitAI	01.08.2026	Nach Abschlussbericht
Frist KI-VO (Art. 113)	**02.08.2026**	**KRITISCH**

2D — CreditVision Score: Konformitätsprüfung

Meilenstein	Frist	Status (März 2026)
BaFin-Stellungnahme	15.05.2026	In Vorbereitung
Audit-Start Hagedorn	Mai 2026	Geplant
Art. 22 DSGVO Prozess-Härtung	30.04.2026	In Umsetzung
Bias-Tests CreditVision	30.06.2026	Nachforderung
DPIA (falls erforderlich)	30.06.2026	Prüfung läuft
Konformitätsbewertung Abschlussbericht	31.07.2026	Geplant
EU-Datenbank-Registrierung	01.08.2026	Nach Abschlussbericht
Frist KI-VO (Art. 113)	**02.08.2026**	**KRITISCH**

Phase 3: Konsolidierung (Januar–Dezember 2027)

Meilenstein	Frist
Jährliche Bias-Test-Überprüfung alle Systeme	Q2 2027
Aktualisierung KI-Inventar (neue Systeme 2026/2027)	Q1 2027
Überprüfung PredictMaint (Art. 6, Anh. I)	01.08.2027
Governance-Leitlinie v3 (Anpassung nach Erfahrungen Phase 2)	Q1 2027

Meilenstein	Frist
GPAI-Modell-Compliance Review (OpenAI-Verträge)	Q2 2027
Zweiter interner Audit KI-Compliance	Q3 2027
Aufsichtsratsbericht Phase-3-Start	Dez. 2026

3. Ampel-Übersicht (März 2026)

Thema	Status
KI-Inventar	■ Grün
Risikoklassifikation	■ Grün
Art. 5 Verbote	■ Grün
Art. 50 Transparenz (ServiceBot)	■ Grün
AI Literacy gesamt	■ Gelb (38 %)
AI Literacy HR / Finanzierung	■ Rot (unter 40 %)
RecruitAI Konformitätsprüfung	■ Rot (Bias-Tests fehlen)
CreditVision Score Konformitätsprüfung	■ Gelb (BaFin-Anfrage offen)
Betriebsvereinbarung	■ Rot (keine Einigung)
Vendor-Verträge KI-VO	■ Gelb
DPIA RecruitAI	■ Gelb (Entwurf läuft)
Schatten-KI Marketing	■ Grün (abgeschaltet, Aufarbeitung)

Aktenzeichen: TI-KI-2026-007. Version 2.0. Verfasser: Dr. F. Roosendaal, A. Kühnhausen. Stand: März 2026.

Datei: 21-budgetplan-governance-funktion.md

Budgetplan — KI-Governance-Funktion Thalheim Industries SE 2026/2027

Aktenzeichen: TI-KI-2026-007

Dokumentversion: 1.2

Erstellungsdatum: 20. Oktober 2025 (aktualisiert März 2026)

Verfasser: Klaus-Dieter Obermaier (CFO); Annegret Kühnhausen (CCO)

Freigabe: Vorstand VS-2025-087 (15.10.2025); Aktualisierung durch KI-Komitee 14.03.2026

1. Übersicht Programmbudget TI-KI-2026

Das Gesamtbudget des Programms TI-KI-2026 (Phase 1 und 2) wurde durch den Vorstand am 15.10.2025 mit 1.450.000 EUR genehmigt. Auf Basis der Erkenntnisse aus Phase 1 und den Eskalationsthemen Q1 2026 wird ein Nachtragsbudget von 215.000 EUR beantragt (vgl. Eskalationsvorlage Aktenstück 17).

Gesamtbudget inkl. Nachtrag: 1.665.000 EUR

2. Budgetplan nach Kostenstellen

2.1 Externe Rechtsberatung

Position	Budget 2025	Budget 2026	Budget 2027	Gesamt
Kanzlei Borchmann Compliance (Rahmenmandat)	15.000 EUR	195.000 EUR	70.000 EUR	280.000 EUR
Synaptec-Vertragsdurchsetzung (Nachtrag)	—	50.000 EUR	—	50.000 EUR
BaFin-Stellungnahme (inbegriffen Borchmann)	—	—	—	0 EUR
Teilsomme Rechtsberatung	**15.000 EUR**	**245.000 EUR**	**70.000 EUR**	**330.000 EUR**

2.2 Externe Prüfung / Audit

Position	Budget 2025	Budget 2026	Budget 2027	Gesamt
WPG Hagedorn & Partner (RecruitAI + CreditVision Score)	—	190.000 EUR	—	190.000 EUR
Unabhängige Bias-Tests (extern, Nachtrag)	—	80.000 EUR	—	80.000 EUR
Jährlicher KI-Compliance-Audit 2027	—	—	90.000 EUR	90.000 EUR
Teilsomme Prüfung/Audit	**0 EUR**	**270.000 EUR**	**90.000 EUR**	**360.000 EUR**

2.3 AI Literacy / Schulung

Position	Budget 2025	Budget 2026	Budget 2027	Gesamt
E-Learning-Plattform-Lizenz (TalentHub KI-Module)	12.000 EUR	45.000 EUR	38.000 EUR	95.000 EUR
Externe Schulungsdienstleister (Präsenz-Workshops)	—	68.000 EUR	20.000 EUR	88.000 EUR
Erstellung Schulungsmaterial (intern + extern)	5.000 EUR	30.000 EUR	10.000 EUR	45.000 EUR
Teilsomme Schulung	**17.000 EUR**	**143.000 EUR**	**68.000 EUR**	**228.000 EUR**

2.4 Technologie und Systemanpassungen

Position	Budget 2025	Budget 2026	Budget 2027	Gesamt
Technische Sperre automatische Ablehnung (RecruitAI)	—	12.000 EUR	—	12.000 EUR
KI-Inventar-Tool (Lizenz + Integration)	8.000 EUR	20.000 EUR	15.000 EUR	43.000 EUR
API-Blocking-Maßnahmen (Schatten-KI-Prävention)	—	18.000 EUR	—	18.000 EUR
Override-Dokumentation in SAP SuccessFactors	—	25.000 EUR	5.000 EUR	30.000 EUR
KI-Dashboard Compliance-Monitoring	—	35.000 EUR	17.000 EUR	52.000 EUR
Teilsomme Technologie	**8.000 EUR**	**110.000 EUR**	**37.000 EUR**	**155.000 EUR**

2.5 Personalaufwand (intern, kalkuliert)

Position	Budget 2025	Budget 2026	Budget 2027	Gesamt
KI-Komitee-Vorsitz Dr. Roosendaal (60 % Kapazität)	28.000 EUR	120.000 EUR	80.000 EUR	228.000 EUR
DSB Dr. Eichenmüller (KI-Anteil, 30 % Kapazität)	12.000 EUR	68.000 EUR	45.000 EUR	125.000 EUR
CCO-Bereich KI-Compliance (1,5 FTE)	18.000 EUR	180.000 EUR	99.000 EUR	297.000 EUR

Position	Budget 2025	Budget 2026	Budget 2027	Gesamt
Teilsomme Personal	**58.000 EUR**	**368.000 EUR**	**224.000 EUR**	**650.000 EUR**

2.6 Nachtrag Eskalation (Vorstandsgenehmigung ausstehend)

Position	2026
Synaptec-Vertragsdurchsetzung (Rechtsberatung)	50.000 EUR
Alternativsystem-Evaluation Recruiting	120.000 EUR
Einigungsstelle BetrVG (geschätzt)	45.000 EUR
Nachtrags-Gesamt	**215.000 EUR**

3. Zusammenfassung

Kategorie	Gesamt 2025–2027
Externe Rechtsberatung	330.000 EUR
Externe Prüfung/Audit	360.000 EUR
AI Literacy / Schulung	228.000 EUR
Technologie	155.000 EUR
Personal (intern kalkuliert)	650.000 EUR
Genehmigtes Gesamtbudget	**1.450.000 EUR** (ohne Nachtrag)
Nachtragsbudget	215.000 EUR
Gesamt inkl. Nachtrag	**1.665.000 EUR**

4. Budgetkontrolle

Periode	Geplant	Verbraucht	Abweichung
Phase 1 (Okt–Dez 2025)	98.000 EUR	91.000 EUR	+7.000 EUR
Q1 2026 (Jan–März 2026)	280.000 EUR	246.000 EUR	+34.000 EUR
Q2 2026 (Apr–Jun 2026)	410.000 EUR	Laufend	—

Periode	Geplant	Verbraucht	Abweichung
Q3 2026 (Jul–Sep 2026)	320.000 EUR	Geplant	—

Das Programm liegt leicht unter dem Ursprungsbudget, jedoch wird der Nachtrag für Synaptec-Eskalation, Einigungsstelle und System-Evaluation benötigt.

Aktenzeichen: TI-KI-2026-007. Verfasser: K.-D. Obermaier, A. Kühnhausen. Stand: März 2026.

Datei: 22-abschlussbericht-projektphase-1.md

Abschlussbericht Projektphase 1 — KI-Governance-Programm TI-KI-2026

Aktenzeichen: TI-KI-2026-007
Dokumentversion: 1.0 (Endfassung)
Berichtszeitraum: Oktober 2025 – Dezember 2025
Datum: 15. Januar 2026
Verfasser: Dr. Falk Roosendaal, KI-Komitee-Vorsitz
Freigegeben durch: Vorstand Thalheim Industries SE (Per-Umlaufbeschluss 20.01.2026)

1. Zusammenfassung

Die Projektphase 1 des KI-Governance-Programms TI-KI-2026 (Oktober–Dezember 2025) ist erfolgreich abgeschlossen. Die Kernziele — vollständige Inventarisierung aller KI-Systeme, Risikoklassifikation nach KI-VO und umfassende Gap-Analyse — wurden in vollem Umfang erreicht. 23 KI-Systeme wurden identifiziert und klassifiziert. Zwei Systeme wurden als Hochrisiko-Systeme eingestuft, die einer vollständigen Konformitätsprüfung bis 02.08.2026 bedürfen.

Die Phase 1 legte damit das Fundament für Phase 2 (Konformitätsherstellung, Januar–Juli 2026) und Phase 3 (Konsolidierung, 2027).

2. Zielerreichung Phase 1

Ziel	Ergebnis	Bewertung
KI-Inventar vollständig	23 Systeme erfasst	✓ Vollständig
Risikoklassifikation	2 Hochrisiko, 3 begrenzt, 1 minimal, 17 weitere	✓ Vollständig
Gap-Analyse je System	Durchgeführt für alle 5 Kernsysteme	✓ Vollständig
Governance-Struktur etabliert	KI-Komitee eingerichtet, Rollen besetzt	✓ Vollständig

Ziel	Ergebnis	Bewertung
KI-Governance-Leitlinie Entwurf	Version 2.0 vorgelegt	✓ Vollständig
Externe Berater mandatiert	Borchmann Compliance + Hagedorn & Partner	✓ Vollständig
Vorstandsbeschluss und Auftrag	VS-2025-087 vom 15.10.2025	✓ Vollständig
Erste Compliance-Maßnahmen (Art. 50, Art. 5)	ServiceBot-Hinweis, Rote Liste	✓ Vollständig
Betriebsrat erste Kontaktaufnahme	Informationsschreiben 20.11.2025	✓ Erledigt

3. Wesentliche Erkenntnisse aus Phase 1

3.1 Zwei Hochrisiko-Systeme mit unmittelbarem Handlungsbedarf

RecruitAI und CreditVision Score sind eindeutig als Hochrisiko nach Anhang III KI-VO einzustufen. Beide Systeme sind bereits im Echtbetrieb. Die Konformitätsherstellung ist bis 02.08.2026 zwingend; ein Betrieb ohne Konformitätsnachweis nach diesem Datum ist gesetzeswidrig.

3.2 Schatten-KI als latentes Risiko erkannt

Die Bestandsaufnahme hat gezeigt, dass mehrere Fachbereiche KI-Tools nutzen, ohne diese zu melden. Der Freigabeprozess war unbekannt oder wurde als nicht relevant eingestuft. Dies wurde als systemisches Risiko eingestuft und mit erhöhter Dringlichkeit in Phase 2 adressiert. (Die tatsächliche Entdeckung eines nicht genehmigten Tools in Marketing erfolgte erst März 2026, bestätigte aber die Phase-1-Risikoeinschätzung.)

3.3 AI Literacy-Pflicht (Art. 4 KI-VO) seit August 2025 bereits anwendbar

Die Inventarisierung ergab, dass die Schulungspflicht nach Art. 4 KI-VO bereits seit 02.08.2025 gilt. Zum Zeitpunkt der Inventarisierung (Oktober 2025) hatte noch kein Mitarbeitender eine formale KI-Literacy-Schulung erhalten. Dies bedeutete einen Rückstand von mehreren Monaten.

3.4 Vendor-Dokumentation systematisch unvollständig

Keiner der drei externen Vendoren (Synaptec, CreditVision AG, OpenAI) hatte zum Zeitpunkt der Inventarisierung vollständige KI-VO-konforme Dokumentation vorgelegt. Dies ist ein Branchen-Pattern, keine Thalheim-spezifische Ausnahme.

3.5 Betriebsrat: Mitbestimmungsrechte frühzeitig einzubeziehen

Der Betriebsrat hat sofort nach erster Kontaktaufnahme (November 2025) auf seine Mitbestimmungsrechte nach § 87 BetrVG hingewiesen. Die Betriebsvereinbarungsverhandlungen wurden als zentrales Projekt für Phase 2 identifiziert.

4. Lessons Learned

Erkenntnis	Empfehlung für Phase 2
KI-Systeme werden ohne Governance-Prozesse eingesetzt	Technische Zugangsbeschränkungen + Freigabeprozess implementieren
Vendor-Dokumentation ist branchenweit unvollständig	Vertragliche Dokumentationspflichten einfordern, SLA einbauen
Art. 4 KI-VO gilt bereits — Schulungsrückstand ist real	AI Literacy als Top-Priorität Phase 2
Betriebsrat ist Schlüsselakteur	Früh und offen einbeziehen; BV-Verhandlung zügig führen
Bias-Tests werden von Vendors nicht proaktiv geliefert	Eigeninitiative: Unabhängige Tests beauftragen
DPIA-Pflicht kann Behörden-Anfrage auslösen	DPIA frühzeitig beginnen, nicht abwarten

5. Übergabe an Phase 2

Phase 2 (Konformitätsherstellung) beginnt am 15. Januar 2026 mit der Konformitätsprüfung RecruitAI durch Hagedorn & Partner. Dr. Roosendaal übernimmt die Projektsteuerung Phase 2. Das KI-Komitee tagt quartalsweise. Nächster Bericht an Vorstand und Aufsichtsrat: Mai 2026 (vgl. Aktenstück 12).

Die vollständige Projektdokumentation Phase 1 umfasst:

- Aktenstücke 01–09 (Governance-Rahmen, Klassifikation, Pflichtenmatrix)
- KI-Inventar (vollständig, 23 Systeme)
- Vendor-Übersichten
- Vertragsregister KI-Systeme
- Protokolle KI-Komitee Q4 2025

6. Dank

Dr. Roosendaal dankt dem Projekt-Core-Team für die intensive Arbeit in Phase 1: Marcus Petersen (CDO), Barbara Trenkmann (HR-Systeme), Rolf Haselmann (Kundenfinanzierung), Dr. Carla Eichenmüller (DSB), IT-Security-Team und der Kanzlei Borchmann Compliance für die kompetente externe Begleitung.

Abschlussbericht Phase 1. Aktenzeichen: TI-KI-2026-007. Verfasser: Dr. F. Roosendaal. Freigabe: Vorstand 20.01.2026.

E-Mails

Datei: email-bafin-anfrage-kreditscoring.eml

Von	GZ-BJ24K7102@bafin.de
An	annegret.kuehnhausen@thalheim-industries.de
Datum	Tue, 10 Mar 2026 09:30:00 +0100
Betreff	Bundesanstalt für Finanzdienstleistungsaufsicht — Anfrage nach § 44 KWG i.V.m. Art. 43 KI-VO — Ihr Kreditscoring-Modul CreditVision Score — GZ BJ 24-K 7102-2026/0012

Von: Bundesanstalt für Finanzdienstleistungsaufsicht
Referat BJ 24 — KI und Digitale Innovation
GZ: BJ 24-K 7102-2026/0012
An: Thalheim Industries SE, z. Hd. Annegret Kühnhausen (CCO)
annegret.kuehnhausen@thalheim-industries.de
CC: Dr. Sigrid Wolfsbacher (CIO)
Datum: 10. März 2026
Betreff: Anfrage zu CreditVision Score — KI-VO und DSGVO Art. 22

Sehr geehrte Frau Kühnhausen,

die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nimmt im Rahmen ihrer Aufgaben nach § 44 KWG sowie als zuständige nationale Behörde für die Aufsicht über Kreditinstitute und vergleichbare Unternehmen die aufsichtliche Prüfung der Konformität automatisierter Kreditentscheidungssysteme mit der Verordnung (EU) 2024/1689 (KI-Verordnung) und der Datenschutz-Grundverordnung vor.

Nach unseren Erkenntnissen setzt die Thalheim Industries SE in Ihrer Kundenfinanzierungseinheit das System CreditVision Score (CreditVision AG, Frankfurt) zur Bonitätsbewertung von Privat- und Gewerbekunden ein.

Wir bitten Sie, zu folgenden Fragen bis zum 15. Mai 2026 schriftlich Stellung zu nehmen:

Frage 1 — Art. 22 DSGVO:

Wie stellt Thalheim Industries SE sicher, dass Kunden, deren Kreditantrag maßgeblich auf Basis von CreditVision Score bewertet wird, ihre Rechte nach Art. 22 DSGVO (Widerspruchsrecht gegen automatisierte Einzelentscheidungen, Recht auf Erläuterung der maßgeblichen Faktoren) vollständig wahrnehmen können? Welche Informationspflichten wurden implementiert?

Frage 2 — Art. 43 Abs. 2 KI-VO:

Hat Thalheim Industries SE die interne Konformitätsbewertung für CreditVision Score nach Art. 43 Abs. 2 KI-VO durchgeführt? Falls ja: Liegt ein Bericht vor, der zur Einsichtnahme bereitgestellt werden kann? Falls nein: Welcher Zeitplan ist für die Durchführung vorgesehen?

Frage 3 — Art. 9 Abs. 7 KI-VO (Bias-Tests):

Wurden für CreditVision Score Bias-Tests durchgeführt, die die Einhaltung von Art. 9 Abs. 7 KI-VO (Erkennung und Minimierung verzerrter Ausgaben) belegen? Bitte legen Sie entsprechende Nachweise oder Erklärungen des Vendors vor.

Die BaFin weist darauf hin, dass bei Nichtbeantwortung oder unvollständiger Beantwortung aufsichtsrechtliche Maßnahmen nach § 6 Abs. 3 KWG eingeleitet werden können.

Für Rückfragen wenden Sie sich bitte an:

Referatsleitung BJ 24 — KI und Digitale Innovation
Bundesanstalt für Finanzdienstleistungsaufsicht
Marie-Curie-Straße 24–28 | 60439 Frankfurt am Main
T: +49 228 4108-0 | bafin@bafin.de

Mit freundlichen Grüßen

Im Auftrag

[Referatsleiterin BJ 24, Name geschwärzt]
Bundesanstalt für Finanzdienstleistungsaufsicht

Datei: email-betriebsrat-mitbestimmung.eml

Von	norbert.schaefers@thalheim-betriebsrat.de
An	annegret.kuehnhausen@thalheim-industries.de
Datum	Mon, 05 Jan 2026 10:14:35 +0100
Betreff	Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG — KI-Systeme RecruitAI und CreditVision Score — Formelle Geltendmachung

Von: Norbert Schäpers <norbert.schaefers@thalheim-betriebsrat.de>
An: Annegret Kühnhausen, CCO <annegret.kuehnhausen@thalheim-industries.de>
CC: Dr. Falk Roosendaal <falk.roosendaal@thalheim-industries.de>;
Betriebsrat Thalheim <betriebsrat@thalheim-industries.de>
Datum: 05. Januar 2026, 10:14 Uhr
Betreff: Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG — KI-Systeme RecruitAI und CreditVision Score
Aktenzeichen BR: BR-2026-001

Sehr geehrte Frau Kühnhausen,

der Betriebsrat der Thalheim Industries SE macht hiermit formell sein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) geltend.

Nach § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, mitzubestimmen bei Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind oder geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

Unsere Auffassung:

Bei RecruitAI handelt es sich um ein System, das Bewerberdaten auswertet und Personalentscheidungen beeinflusst. Bei CreditVision Score werden Daten verarbeitet, die — soweit Thalheim-Beschäftigte betroffen sein könnten — ebenfalls der Mitbestimmung unterliegen. Beide Systeme sind zudem nach der EU-KI-Verordnung als Hochrisiko-Systeme eingestuft.

Konsequenz:

Der Betriebsrat verweigert seine Zustimmung zum Weiterbetrieb dieser Systeme, bis eine Betriebsvereinbarung nach § 87 BetrVG abgeschlossen ist. Wir erwarten die Aufnahme von Verhandlungen bis spätestens 30. Januar 2026.

Anforderungen des Betriebsrats:

1. Vollständige Transparenz über die Algorithmus-Logik beider Systeme (in verständlicher Sprache).
2. Recht auf Hinzuziehung externer Sachverständiger auf Kosten des Arbeitgebers (§ 80 Abs. 3 BetrVG).
3. Regelmäßige Berichterstattung über Bias-Testergebnisse an den Betriebsrat.

4. Klares Recht jeder Mitarbeiterin und jedes Mitarbeiters auf Erklärung KI-basierter Entscheidungen.
5. Verbot vollautomatischer Ablehnungen ohne menschliche Überprüfung.

Ich bitte um Eingangsbestätigung bis 09. Januar 2026 und um Terminvorschlag für das erste Verhandlungsgespräch bis 30. Januar 2026.

Mit freundlichen Grüßen

Norbert Schäpers
Betriebsratsvorsitzender | Thalheim Industries SE
T: +49 621 9340-2800
norbert.schaefers@thalheim-betriebsrat.de

Anlage: Stellungnahme des DGB-Rechtsbüros zu KI-Systemen und § 87 BetrVG (liegt für Rückfragen vor)

Datei: email-cio-an-vorstand-projektstart.eml

Von	sigrid.wolfsbacher@thalheim-industries.de
An	vorstand@thalheim-industries.de
Datum	Thu, 09 Oct 2025 08:42:17 +0200
Betreff	AW: KI-Verordnung EU 2024/1689 — Dringender Handlungsbedarf — Projektstart TI-KI-2026

Von: Dr. Sigrid Wolfsbacher <sigrid.wolfsbacher@thalheim-industries.de>
An: Vorstand Thalheim Industries SE <vorstand@thalheim-industries.de>
CC: Annegret Kühnhausen <annegret.kuehnhausen@thalheim-industries.de>;
Dr. Falk Roosendaal <falk.roosendaal@thalheim-industries.de>
Datum: 09. Oktober 2025, 08:42 Uhr
Betreff: KI-Verordnung EU 2024/1689 — Dringender Handlungsbedarf — Projektstart TI-KI-2026

Sehr geehrte Damen und Herren im Vorstand,

ich wende mich mit dieser E-Mail direkt an den Vorstand, da die Sache keinen weiteren Aufschub duldet.

Hintergrund:

Die Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-VO) tritt mit gestaffelten Fristen in Kraft. Für Hochrisiko-KI-Systeme nach Art. 6 i.V.m. Anhang III KI-VO gilt die vollständige Anwendungsfrist ab dem 02. August 2026. Thalheim Industries SE betreibt mindestens zwei solcher Systeme: RecruitAI (Synaptec Analytics GmbH) und CreditVision Score (CreditVision AG).

Was das bedeutet:

Ohne vollständige Konformitätsprüfung (Art. 43 KI-VO) und Registrierung in der EU-Datenbank (Art. 49 KI-VO) dürfen wir diese Systeme nach dem 02.08.2026 nicht mehr betreiben.
Bußgelder: bis zu 15 Mio. EUR oder 3 % des Jahresumsatzes (Art. 99 KI-VO).

Zur Erinnerung an den Kontext:

Zusätzlich hat die KI-VO bereits seit dem 02.08.2025 die Pflicht zur AI Literacy (Art. 4 KI-VO) in Kraft gesetzt. Kein einziger unserer 12.000 Mitarbeitenden hat bislang eine formale Schulung erhalten.

Was ich beantrage:

1. Einrichtung eines Programms TI-KI-2026 mit voller Vorstandsunterstützung und klarer Führung.
2. Budget: 1,45 Mio. EUR für Phase 1 und 2 (Inventarisierung + Konformitätsherstellung).
3. Benennung Dr. Falk Roosendaal als KI-Komitee-Vorsitz.
4. Mandatierung externer Rechtsberatung (Borchmann Compliance) und Auditor (Hagedorn & Partner).

Ich bitte, diesen Punkt auf die Vorstandssitzung am 15.10.2025 zu setzen.

Ich stehe für Rückfragen jederzeit zur Verfügung.

Mit besten Grüßen

Dr. Sigrid Wolfsbacher
Chief Information Officer | Thalheim Industries SE
August-Bebel-Ring 14 | 68163 Mannheim
T: +49 621 9340-1100 | M: +49 173 8801237
sigrid.wolfsbacher@thalheim-industries.de

Vertraulichkeitshinweis: Diese E-Mail und ihre Anhänge sind vertraulich und ausschließlich für den oben genannten Empfänger bestimmt. Wenn Sie diese E-Mail versehentlich erhalten haben, benachrichtigen Sie bitte den Absender und löschen Sie die E-Mail.

Datei: email-konzernrevision-feststellungen.eml

Von	franz-josef.brammer@thalheim-industries.de
An	annegret.kuehnhausen@thalheim-industries.de
Datum	Sat, 14 Mar 2026 16:08:42 +0100
Betreff	DRINGEND: Revisionsfeststellung — Nicht genehmigtes KI-Tool Marketingabteilung (Schatten-KI) — INC-2026-003

Von: Franz-Josef Brammer, Leiter Konzernrevision
<franz-josef.brammer@thalheim-industries.de>
An: Annegret Kühnhausen (CCO) <annegret.kuehnhausen@thalheim-industries.de>;
Dr. Reinhard Thalheim-Lattermann (CEO) <reinhard.thalheim-lattermann@thalheim-industries.de>
CC: Dr. Sigrid Wolfsbacher (CIO); Marcus Petersen (CDO); Dr. Carla Eichenmüller (DSB)
Datum: 14. März 2026, 16:08 Uhr
Betreff: DRINGEND — Schatten-KI Marketingabteilung — INC-2026-003
Klassifizierung: VERTRAULICH — NUR VORSTAND UND KI-KOMITEE

Sehr geehrte Frau Kühnhausen, sehr geehrter Herr Dr. Thalheim-Lattermann,

ich melde hiermit eine kritische Revisionsfeststellung gemäß § 5 der Revisionsordnung und Art. 26 Abs. 4 KI-VO.

Sachverhalt (Stand heute, 14.03.2026, 15:30 Uhr):

Im Rahmen der laufenden KI-Compliance-Prüfung hat die Konzernrevision festgestellt, dass die Marketingabteilung (Leiter: Dr. Philipp Sonntag) seit mindestens Juli 2025 das KI-Tool Midjourney (Bildgenerierung, Basismodell Midjourney Inc., USA) über eine nicht genehmigte API-Anbindung auf einem selbst eingerichteten Server einsetzt.

Konkrete Feststellungen:

1. Das Tool ist NICHT im zentralen KI-Inventar eingetragen.
2. Es existiert KEINE Datenschutzprüfung für dieses System.
3. Es existiert KEINE Sicherheitsfreigabe durch IT-Security.
4. KEINE Genehmigung durch CCO oder CDO liegt vor.
5. Erste Analyse der API-Nutzungsprotokolle (Cloud-Kostenabrechnung): ca. 2.400 API-Aufrufe seit Juli 2025. In mindestens 34 Aufrufen wurden Kundennamen und Firmennamen in Prompts eingegeben — diese Daten wurden an Server der Midjourney Inc. in den USA übermittelt (Drittlandtransfer ohne Rechtsgrundlage, Art. 44 ff. DSGVO potenziell verletzt).

Sofortmaßnahme:

Ich empfehle dringend, das System SOFORT durch IT abschalten zu lassen. Ich bitte um Ihre

Genehmigung für diese Maßnahme bis heute 18:00 Uhr.

Dr. Sonntag wurde noch nicht informiert; ich empfehle, dies nach der IT-Abschaltung zu tun (Sicherstellung der Protokollsicherung zuerst).

Datenschutzrechtliche Konsequenzen:

DSB Dr. Eichenmüller muss unverzüglich prüfen, ob eine Meldepflicht nach Art. 33 DSGVO besteht.

Ich stehe für ein Kurzgespräch heute Abend oder morgen früh zur Verfügung.

Mit freundlichen Grüßen

Franz-Josef Brammer

Leiter Konzernrevision | Thalheim Industries SE

T: +49 621 9340-3300 | M: +49 162 7741892

franz-josef.brammer@thalheim-industries.de

VERTRAULICH. Diese E-Mail enthält revisionsinterne Informationen. Nicht weiterzuleiten.

Datei: email-openai-vendor-zertifizierung.eml

Von	enterprise-eu@openai.com
An	marcus.petersen@thalheim-industries.de
Datum	Wed, 18 Mar 2026 14:22:06 +0100
Betreff	RE: EU AI Act Compliance Documentation Request — Enterprise Account OAI-ENT-2024-TI-0892

Von: OpenAI Ireland Ltd., Enterprise Compliance Team

<enterprise-eu@openai.com>

An: Marcus Petersen, CDO Thalheim Industries SE

<marcus.petersen@thalheim-industries.de>

CC: Annegret Kühnhausen <annegret.kuehnhausen@thalheim-industries.de>

Datum: 18. März 2026, 14:22 Uhr

Betreff: RE: EU AI Act Compliance Documentation — Ihr Schreiben vom 15.02.2026

Ihr Ref.: TI-CDO-2026-0041 | Unser Ref.: OAI-COMP-EU-2026-1847

Sehr geehrter Herr Petersen,

vielen Dank für Ihre Anfrage vom 15. Februar 2026 bezüglich der EU AI Act Compliance-Dokumentation für Ihren Enterprise-Vertrag OAI-ENT-2024-TI-0892.

Wir nehmen die Anforderungen des EU AI Acts sehr ernst und arbeiten intensiv an der vollständigen Dokumentation für unsere Enterprise-Kunden.

Status Ihrer Anfragen:

Anfrage 1 — Produktspezifische technische Dokumentation:

Wir verweisen auf unsere EU-AI-Act-Compliance-Seite: <https://openai.com/eu-ai-act>

Für produktspezifische Dokumentation Ihrer CodeAssist-Deployment-Konfiguration können wir derzeit keine separaten Dokumente bereitstellen. Unser Enterprise-Team arbeitet an einem standardisierten Deployment-Dokumentationspaket, das voraussichtlich im Q3 2026 verfügbar sein wird.

Anfrage 2 — Trainingsdaten-Zusammenfassung:

Die Zusammenfassung der Trainingsdaten für GPT-4o ist in unserem System Card verfügbar:

<https://openai.com/research/gpt-4o-system-card>

Eine spezifischere Aufschlüsselung können wir aus proprietären Gründen nicht bereitstellen.

Anfrage 3 — Known Limitations / Bias Disclosure:

Bekannte Schwächen und Bias-Kategorien sind im System Card (s.o.) dokumentiert.

Anfrage 4 — Incident Notification SLA:

Unser Standard-SLA für Sicherheitsvorfallmeldungen beträgt 72 Stunden für kritische Incidents.

Für eine spezifische vertragliche Anpassung auf 24 Stunden bitten wir um eine formelle Anfrage über Ihren Enterprise Account Manager.

Anfrage 5 — Systemisches Risiko GPT-4o:

OpenAI hat GPT-4o als GPAI-Modell mit systemischem Risiko im Sinne von Art. 51 KI-VO eingestuft.

Die entsprechenden Maßnahmen nach Art. 55 KI-VO (u.a. Adversarial Testing) werden durchgeführt und dokumentiert. Weitere Informationen folgen im Rahmen unserer GPAI Code of Practice Implementierung.

Wir bitten um Verständnis, dass die Umsetzung der EU AI Act Anforderungen für GPAI-Anbieter noch in Entwicklung ist. Wir werden Sie über Aktualisierungen informieren.

Mit freundlichen Grüßen

Sarah O'Connor

Enterprise Compliance Lead, EMEA

OpenAI Ireland Ltd.

2 Grand Canal Square, Dublin 2, Ireland

enterprise-eu@openai.com

Hinweis: OpenAI Ireland Ltd. ist ein Tochterunternehmen von OpenAI, LLC und verarbeitet Daten von Enterprise-Kunden in der EU gemäß den Bedingungen unseres Enterprise Datenschutz-Abkommens.

Excel-Tabellen

Datei: pflichtenmatrix-art-9-ff-kivo.xlsx

Tabellenblatt: Pflichtenmatrix Art. 9 ff.

	<div>Pflichtenmatrix Art. 9 ff. KI-VO — Hochrisiko-Systeme Thalheim Industries SE TI-KI-2026-009 Stand: März 2026</div>									
	<div>Legende: ✓ = erfüllt ■ = teilweise / in Bearbeitung ✗ = nicht erfüllt — = nicht anwendbar Rechtsgrundlage: Art. 9–17 KI-VO; Art. 26 KI-VO; Art. 35 DSGVO; Art. 22 DSGVO</div>									
	KI-System	Art. 9 Risikomanagement	Art. 9 Abs. 7 Bias-Tests	Art. 10 Datenqualität	Art. 11 Techn. Dokumentation	Art. 12 Protokollierung	Art. 13 Transparenz	Art. 14 Mensch. Aufsicht	Art. 15 Genauigkeit/Cybers.	Art. 43 Konformitätsbew.
	RecruitAI (Hochrisiko, Anh. III 4a)	■ In Bearbeitung	✗ FEHLT — kritisch	■ Teilweise	■ Nachforderung läuft	✓ Aktiviert	✓ Gebrauchsanweisung DE	■ Konzept, SOP fehlt	■ Pentest ausstehend	■ Audit läuft

	CreditVision Score (Hochrisiko, Anh. III 5b)	■ Entwurf Vendor	■ Unklar — angefordert	■ In Prüfung	■ Teilweise geliefert	✓ Aktiviert	✓ DE + EN	✓ Letzte Entscheidung HR	■ ISO 27001 CV-AG	■ Audit geplant Mai
	Predict Maint (Begrenztes Risiko)	— Nicht Hochrisiko	— Nicht Hochrisiko	■ Intern dokumentiert	✓ Intern vollständig	✓ Logs vorhanden	— Kein Konsum . direkt	— Kein Personenbezug	✓ Interne Tests OK	— Nicht erforderlich
	CodeAssist / GPT-4o (Begrenztes Risiko, GPAI)	— Deployer-Pflichten	— Nicht Hochrisiko	✓ Nutzungsrichtlinie	■ Vendor-Dokument. unvollst.	— Plattformseitig	■ Kennzeichnung prüfen	✓ Mensch reviewt Code	✓ SOC 2 Type II	— Nicht erforderlich
	Service Bot (Transparenzpflichten)	— Kein Hochrisiko	— Kein Hochrisiko	— Keine Personendaten	✓ Intern dokumentiert	✓ Aktiviert	✓ Art. 50-Hinweis aktiv	— Eskalation zu Mensch	✓ Intern getestet	— Nicht erforderlich
	MarketingAI / Midjourney (Schatten-KI — abgeschaltet)	✗ Keine Dokumentation	— Nicht klassifiziert	✗ Keine Datenschutzprüfung	✗ Kein Vendor-Nachweis	✗ Keine Protokolle	✗ Keine Offenlegung	✗ Keine Aufsicht	✗ Keine Sicherheitsprüfung	✗ Keine Bewertung
	HRAnalytics (Workday)	— Prüfung läuft	— BetrVG-Prüfung	■ Aggregatdaten prüfen	■ Workday-Doku angefor.	✓ Workday-seitig	■ DSB-Prüfung läuft	— Aggregatdaten	✓ ISO 27001 Workday	— Prüfung folgt
	ChurnPredictor (Salesforce CRM)	— Kein Hochrisiko	— Kein Hochrisiko	✓ Datenschutzprüfung OK	✓ Salesforce-Doku vorl.	✓ Salesforce-Logs	■ Art. 21 DSGVO prüfen	— B2B-Kontext	✓ SOC 2 Salesforce	— Nicht erforderlich
	FraudDetector (Intern)	— Prüfung läuft	— Prüfung läuft	■ Interne Transaktions-D.	■ In Erarbeitung	✓ ERP-Logs	■ Beschäftigte informieren.	■ Letzte Entscheidung CFO	✓ Interne Prüfung	— Prüfung folgt
	AutoTranslate (DeepL)	— Minimales Risiko	— Minimales Risiko	✓ Keine Personendaten im Normalbetrieb	✓ DeepL-Doku ausreichend	— Plattformseitig	— Kein Konsum . direkt	— Keine Entscheidungen	✓ DeepL DSGVO-konform	— Nicht erforderlich
	Finance Report-AI (Intern)	— Minimales Risiko	— Minimales Risiko	✓ Aggregatdaten	✓ Intern dokumentiert	✓ ERP-Logs	— Interne Berichte	— Keine Personenentscheid.	✓ Intern OK	— Nicht erforderlich
	EmailSorter (MS Copilot)	— Minimales Risiko	— Minimales Risiko	■ Copilot-Datenschutz prüfen	■ MS-Doku angefordert	— Plattformseitig	■ Mitarbeiter informieren	— Assistenz, kein Entscheid	■ MS-Zertifikat anfordern	— Nicht erforderlich

	QualityVision (Intern)	— Kein Hochrisiko	— Kein Hochrisiko	✓ Masc hinendaten	✓ Intern vollständig	✓ Produktions-Logs	—Keine Konsumenten	— Masc hinenbedienung	✓ Intern getestet	— Nicht erforderlich
	EnergyForecast (Intern)	— Mini males Risiko	— Mini males Risiko	✓ Verbrauchsdaten	✓ Intern dokumentiert	✓ Betriebsdaten-Log	—Keine Konsumenten	— Prognosemodell	✓ Intern getestet	— Nicht erforderlich
	PricingOptimizer (Intern)	— Mini males Risiko	— Mini males Risiko	✓ B2B-Preisdaten	✓ Intern dokumentiert	✓ ERP-Log	— B2B, keine Verbraucher	—Keine Personennentscheid.	✓ Intern OK	— Nicht erforderlich
	SupplyChainAI (SAP)	— Mini males Risiko	— Mini males Risiko	✓ Logistikdaten	✓ SAP-Dokumentation	✓ SAP-Logs	—Keine Konsumenten	— Logistik, kein Personennentscheid.	✓ SAP ISO 27001	— Nicht erforderlich
	TenderAnalyzer (SaaS extern)	— Mini males Risiko	— Mini males Risiko	■ B2B; Datenschutz prüfen	■ SaaS-Doku angefor.	— Plattformseitig	— B2B-Ausschreibungen	—Keine Personennentscheid.	■ SaaS-Sicherheitsprüfung	— Nicht erforderlich
	LegalResearchAI (Intern + Lexis Nexis)	— Mini males Risiko	— Mini males Risiko	✓ Keine Personendaten	✓ Lexis Nexis-Doku OK	— Recherchetooll	— Interne Nutzung	— Recherche, kein Entscheid.	✓ Lexis Nexis-Sicherheit OK	— Nicht erforderlich
	SpamFilter (Proofpoint)	— Mini males Risiko	— Mini males Risiko	✓ E-Mail-Metadaten DSGVO	✓ Proofpoint-Doku	✓ Quarantäne-Logs	— IT-intern	— Sicherheitssystem	✓ ISO 27001 Proofpoint	— Nicht erforderlich
	CarbonFootprint AI (Intern)	— Mini males Risiko	— Mini males Risiko	✓ Produktionsdaten	✓ Intern dokumentiert	✓ Produktions-Logs	— ESG-Reporting intern	—Keine Personennentscheid.	✓ Intern OK	— Nicht erforderlich
	DocumentClassifier (Intern)	— Mini males Risiko	— Mini males Risiko	✓ Vertragsdaten DSGVO OK	✓ Intern dokumentiert	✓ Dokumenten-Log	— Interne Nutzung	— Keine abschl. Entscheidung.	✓ Intern OK	— Nicht erforderlich
	MaintenanceScheduler (Intern)	— Mini males Risiko	— Mini males Risiko	✓ Masc hinendaten	✓ Intern vollständig	✓ Betriebsdaten-Log	—Keine Konsumenten	— Wartungsplanung	✓ Intern getestet	— Nicht erforderlich
	CodeReviewer (SonarQube)	— Mini males Risiko	— Mini males Risiko	✓ Quellcode intern	✓ SonarQube-Doku	✓ Review-Logs	— Interne Nutzung	— Entwickler-Tool	✓ SonarQube-Sicherheit OK	— Nicht erforderlich
	VoiceAssistant (Intern)	— Kein Hochrisiko	— Kein Hochrisiko	✓ Sprachbefehle anonym.	✓ Intern dokumentiert	✓ Produktionslogs	— Interne Bedienung	✓ Masc hinenoperator Letztentscheid	✓ Sicherheitsfreigabe	— Nicht erforderlich
	SentimentAnalyzer (Intern)	— Kein Hochrisiko	— Kein Hochrisiko	✓ Anonyme Feedback-Texte	✓ Intern dokumentiert	— Aggregatbewertung	■ Kundenmitteilung prüfen	— Aggregatdaten	✓ Intern OK	— Nicht erforderlich

	Rechtsg rundlage n: Art. 9 KI-VO (h ttps://dej ure.org/ gesetze/ KIVO/9. html); Art. 26 KI-VO (h ttps://dej ure.org/ gesetze/ KIVO/26 .html); Art. 35 DSGVO (https://d ejure.or g/gesetz e/DSGV O/35.ht ml); Art. 22 DSGVO (https://d ejure.or g/gesetz e/DSGV O/22.ht ml). Thal heim Ind ustries SE. Akte nzeiche n: TI-KI- 2026-00 9.								
--	---	--	--	--	--	--	--	--	--

Datei: risikoklassifikation-ki-systeme.xlsx

Tabellenblatt: Risikoklassifikation

Risikokl assifikati on KI-Sy steme — Thalh eim Indu stries SE TI- KI-2026- 008 Stand: März 2026									
---	--	--	--	--	--	--	--	--	--

	KI-System	Geschäftsbereich	Anwendungsfall	KI-VO-Risikoklasse	Begründung (Anh. III)	Verantwortlicher	Konformitätsfrist	Vendor	DPIA erforderlich	Status
	RecruitAI	HR / Personal	Automatisiertes Screening und Ranking von Bewerbungsunterlagen	Hochrisiko	Art. 6 Abs. 2, Anh. III Nr. 4 lit. a KI-VO: Personalauswahl/-priorisierung	Dr. S. Wolfsbacher (CIO)	02.08.2026	Synaptic Analytics GmbH	Ja (Art. 35 DSGVO)	KRITISCH — Bias-Tests fehlen
	CreditVision Score	Kundenfinanzierung	Bonitätsbewertung von Privat- und Gewerbekunden für Kreditentscheidungen	Hochrisiko	Art. 6 Abs. 2, Anh. III Nr. 5 lit. b KI-VO: Kreditwürdigkeitsbewertung	M. Petersen (CDO)	02.08.2026	CreditVision AG	Prüfung läuft	HOCH — BaFin-Anfrage offen
	Predict Maint	Produktion / Anlagenbau	Anomalieerkennung und Verschleißprognose auf Basis von Sensordaten	Begrenztes Risiko	Kein Anh.-III-Tatbestand; keine Personenbezogenheit; wirtschaftliche Relevanz	Dr. S. Wolfsbacher (CIO)	02.08.2027	Intern (Thalheim Digital Lab)	Nein	OK — Inventarisiert
	CodeAssist	Software-Entwicklung	KI-gestützte Code-Generierung und Code-Review (GPT-4o-basiert)	Begrenztes Risiko (GPAI)	Art. 51 ff. KI-VO: Allzweck-KI-Modell; kein Anh.-III-Tatbestand	M. Petersen (CDO)	02.08.2027	OpenAI Ireland Ltd.	Nein	MITTEL — Vendor-Doku unvollständig
	Service Bot	Kundenservice	Automatisierte Beantwortung von Kundenanfragen (First-Level-Support)	Transparenzpflichten	Art. 50 Abs. 1 KI-VO: Konversationssystem; Offenlegungspflicht ggü. Nutzern	M. Petersen (CDO)	02.02.2025	Intern (Thalheim Digital Lab)	Nein	OK — Hinweis implementiert

	MarketingAI (Midjourney)	Marketing	Bildgenerierung für Marketingmaterialien (Basismodell Midjourney)	Begrenztes Risiko	Kein Anh.-III-Tatbestand; GPAI-Nutzung; Schatten-KI identifiziert	A. Kühnhausen (CCO)	02.08.2027	Midjourney Inc. (USA)	Prüfung läuft	KRITISCH — Schatten-KI; abgeschaltet
	AutoTranslate	Konzernintern	Automatische Übersetzung interner Dokumente (DS GVO-neutral)	Minimales Risiko	Kein Anh.-III-Tatbestand; keine erhebliche Personenbezogenheit	M. Petersen (CDO)	Keine Frist	DeepL SE	Nein	OK
	Finance Report-AI	Controlling / Finanzen	Automatisierte Erstellung von Finanzberichten aus ERP-Daten	Minimales Risiko	Keine Personenentscheidungen; nur aggregierte Daten	K.-D. Obermaier (CFO)	Keine Frist	Intern	Nein	OK
	EnergyForecast	Energiemanagement	Verbrauchsprognose und Lastspitzenoptimierung für Werksanlagen	Minimales Risiko	Keine Personenbezogenheit; Betriebssicherheitsrelevanz niedrig	Prof. Dr. Schirrmeyer (COO)	Keine Frist	Intern	Nein	OK
	QualityVision	Qualitätskontrolle	Optische Inspektion von Bauteilen auf Defekte (kamera-basiert)	Begrenztes Risiko	Kein Anh.-III-Tatbestand; keine Personenerkennung; Maschinendaten	Prof. Dr. Schirrmeyer (COO)	02.08.2027	Intern	Nein	OK — Jährliche Überprüfung
	HRAalytics	HR / Personal	Aggregierte Auswertung von Mitarbeiterbefragungen	Begrenztes Risiko	Kein direkt. Anh.-III-Tatbestand; Aggregatdaten; BetrVG § 87 prüfen	Dr. S. Wölfsbacher (CIO)	02.08.2027	Workday Inc.	Prüfung	MITTEL — BetrVG-Prüfung läuft

	ChurnPredictor	Vertrieb / CRM	Abwanderungswahrscheinlichkeit bei Bestandskunden	Begrenztes Risiko	Kundendaten; kein Anhang III-Tatbestand; Art. 21 DSGVO beachten	M. Petersen (CDO)	02.08.2027	Salesforce Inc.	Nein	OK — Datenschutzprüfung erledigt
	PricingOptimizer	Vertrieb / Pricing	Dynamische Preisgestaltung für Standardprodukte	Minimales Risiko	Kein Personenbezug für individuelle Entscheidungen; B2B-Kontext	Prof. Dr. Schirrmeyer (COO)	Keine Frist	Intern	Nein	OK
	SupplyChainAI	Beschaffung	Lieferketten-Optimierung und Bestellprognose	Minimales Risiko	Keine Personenbezogenheit; logistische Daten	Prof. Dr. Schirrmeyer (COO)	Keine Frist	SAP SE	Nein	OK
	DocumentClassifier	Legal / Compliance	Automatische Klassifikation von Vertragsunterlagen	Minimales Risiko	Keine Personenentscheidungen; Dokumentenverarbeitung	A. Kühnhausen (CCO)	Keine Frist	Intern	Nein	OK — Datenschutzprüfung erledigt
	SentimentAnalyzer	Kundenservice	Stimmungsanalyse auf Basis von Kundenfeedback-Texten (aggregiert)	Begrenztes Risiko	Aggregatenauswertung; kein Emotionserkennungst Tatbestand Art. 5 Abs. 1 f	M. Petersen (CDO)	02.08.2027	Intern	Nein	OK — Prüfung abgeschlossen
	MaintenanceScheduler	Anlagenbau / Service	Optimierung von Wartungsplänen auf Basis historischer Ausfallmuster	Minimales Risiko	Reine Maschinendaten; kein Personenbezug	Prof. Dr. Schirrmeyer (COO)	Keine Frist	Intern	Nein	OK

	CarbonFootprint AI	ESG / Nachhaltigkeith	Berechnung und Prognose von CO2-Emissionen je Produktionslinie	Minimales Risiko	ESG-Reporting; keine Personeneinscheidungen	M. Petersen (CDO)	Keine Frist	Intern	Nein	OK
	TenderAnalyzer	Vertrieb / Ausschreibungen	Analyse öffentlicher Ausschreibungen und Angebots-Scoring	Minimales Risiko	B2B; keine personenbezogene Entscheidungen gegenüber Individuen	Prof. Dr. Schirrmeyer (COO)	Keine Frist	Extern (SaaS)	Nein	OK — Datenschutzprüfung geplant
	EmailSorter	Alle Bereiche	KI-gestützte Kategorisierung und Priorisierung interner E-Mails	Minimales Risiko	Personalisierungstool; kein Leistungsmonitoring; kein Art. 5-Tatbestand	M. Petersen (CDO)	Keine Frist	Microsoft 365 Copilot	Nein	MITTEL — Copilot-Datenschutzprüfung ausstehend
	SpamFilter	IT / Sicherheit	Automatische Filterung von Spam- und Phishing-E-Mails	Minimales Risiko	Sicherheitssystem; keine Personeneinscheidungen	Dr. S. Wolfsbacher (CIO)	Keine Frist	Proofpoint Inc.	Nein	OK
	CodeReviewer	Software-Entwicklung	Automatische Code-Qualitätsprüfung (static analysis + AI)	Minimales Risiko	Kein Personalentscheid; Entwickler-Tool; kein Leistungsmonitoring	M. Petersen (CDO)	Keine Frist	SonarQube / intern	Nein	OK
	FraudDetector	Finanzen / Kontrolle	Anomalieerkennung bei internen Finanztransaktionen (Anti-Fraud)	Begrenztes Risiko	Interne Kontrolle; Personenbezug möglich; § 87 BetrVG prüfen	K.-D. Obermaier (CFO)	02.08.2027	Intern	Prüfung	MITTEL — BetrVG-Prüfung läuft

	LegalResearchAI	Legal / Recht	KI-gestützte Recherche in Gesetzestexten und Urteilen	Minimal es Risiko	Reines Recherchewerkzeug; keine Personenentscheidungen	A. Kühnhausen (CCO)	Keine Frist	Intern + LexisNexis	Nein	OK
	VoiceAssistant	Produktion / Service	Sprachsteigerung für Maschinenparameter in der Fertigung	Begrenztes Risiko	Kein Anh.-III-Tatbestand; keine Personenerkennung; Maschinenbedienung	Prof. Dr. Schirrmeyer (COO)	02.08.2027	Intern	Nein	OK — Sicherheit sfreigabe erteilt
	Rechtsg rundlage n: KI-VO Art. 6 i.V.m. Anhang III (https://dejure.org/gesetze/KIV/O/6.html); DSGVO Art. 35 (https://dejure.org/gesetze/DSGVO/35.html); BetrVG § 87 (https://dejure.org/gesetze/BetrVG/87.html). Thalheim Industries SE, KI-Komitee. Aktenzeichen: TI-KI-2026-008.									

Word-Dokumente

Datei: betriebsvereinbarung-ki-entwurf.docx

BETRIEBSVEREINBARUNG

über den Einsatz von KI-Systemen bei der Thalheim Industries SE

ENTWURF Version 0.5 — Verhandlungsstand 08. April 2026 — NICHT UNTERZEICHNET

Parteien

Diese Betriebsvereinbarung wird geschlossen zwischen: der Thalheim Industries SE, August-Bebel-Ring 14, 68163 Mannheim, vertreten durch den Vorstand, CCO Annegret Kühnhausen — nachfolgend 'Arbeitgeber' — und dem Betriebsrat der Thalheim Industries SE, vertreten durch den Vorsitzenden Norbert Schäpers — nachfolgend 'Betriebsrat' —

Präambel

Die Thalheim Industries SE setzt im Rahmen ihrer Geschäftstätigkeit KI-gestützte Systeme ein, darunter Hochrisiko-KI-Systeme im Sinne der Verordnung (EU) 2024/1689 (KI-Verordnung). Der Betriebsrat nimmt sein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG wahr, da KI-Systeme technische Einrichtungen darstellen, die zur Überwachung des Verhaltens oder der Leistung der Arbeitnehmerinnen und Arbeitnehmer bestimmt oder geeignet sein können.

Arbeitgeber und Betriebsrat sind sich einig, dass KI-Systeme nur dann eingesetzt werden dürfen, wenn ihre Funktionsweise transparent, ihre Auswirkungen auf Beschäftigte kalkulierbar und ihr Einsatz mit den Persönlichkeitsrechten der Arbeitnehmerinnen und Arbeitnehmer vereinbar ist.

§ 1 Geltungsbereich

(1) Diese Betriebsvereinbarung gilt für alle KI-Systeme, die: a) Beschäftigtendaten verarbeiten oder auswerten, b) Entscheidungen über Beschäftigte (Einstellung, Beförderung, Leistungsbewertung) unterstützen oder treffen, oder c) Verhaltens- oder Leistungsdaten von Beschäftigten analysieren. (2) Ausdrücklich erfasste Systeme: RecruitAI (Recruiting-Screening), CreditVision Score (soweit Beschäftigte betroffen), HR-Analytics-Tools. (3) Ausdrücklich nicht erfasste Systeme: PredictMaint (keine Beschäftigtendaten), ServiceBot (keine Beschäftigtendaten), CodeAssist (ausschließlich Entwickler-Support).

§ 2 Informations- und Unterrichtungspflichten

(1) Der Arbeitgeber unterrichtet den Betriebsrat vor der Einführung, wesentlichen Änderung oder erstmaligen Nutzung eines KI-Systems im Sinne von § 1 mindestens sechs Wochen vor dem geplanten Einsatz. (2) Die Unterrichtung umfasst mindestens: a) Zweck und Funktionsweise des Systems in verständlicher Sprache; b) Beschreibung der verarbeiteten Datenkategorien; c) Risikoklassifikation nach KI-VO; d) Ergebnis der Datenschutz-Folgenabschätzung (falls durchgeführt); e) Informationen über den Anbieter und bestehende AVV; f) Ergebnis etwaiger Bias-Tests. (3) [Streitpunkt] Der Betriebsrat kann auf Kosten des Arbeitgebers bis zu zwei externe Sachverständige nach § 80 Abs. 3 BetrVG hinzuziehen. [Arbeitgeber: Kostengrenze 10.000 EUR; Betriebsrat: ohne Beschränkung].

§ 3 Zustimmungsvorbehalt

(1) Die Inbetriebnahme von KI-Systemen nach § 1 bedarf der Zustimmung des Betriebsrats. (2) Der Betriebsrat kann die Zustimmung verweigern, wenn: a) die nach § 2 erforderlichen Unterlagen nicht vollständig vorliegen; b) Bias-Tests nicht tolerierbare Diskriminierungsrisiken ergeben haben; c) eine erforderliche DPIA nicht vorliegt oder wesentliche Risiken nicht gemindert wurden; d) die Anforderungen dieser Vereinbarung nicht erfüllt sind. (3) Scheitert die Einigung, ist die Einigungsstelle nach § 76 BetrVG anzurufen.

§ 4 Transparenz und Erklärungsrecht

(1) Beschäftigte, über die ein KI-System Empfehlungen oder Entscheidungen trifft, werden vorab in verständlicher Sprache über den Einsatz des Systems informiert. (2) Beschäftigte haben das Recht, auf Antrag eine Erklärung der Entscheidungsgrundlage zu erhalten (Art. 22 Abs. 3 DSGVO). (3) Vollautomatische Entscheidungen ohne menschliche Überprüfung sind verboten.

§ 5 Menschliche Aufsicht

(1) Bei allen Systemen nach § 1 entscheidet grundsätzlich ein Mensch. Das KI-System ist Entscheidungsunterstützungswerkzeug, kein Entscheidungsträger. (2) Für RecruitAI gilt: Die abschließende Entscheidung liegt beim HR-Business-Partner. Abweichungen vom KI-Ranking sind zu dokumentieren.

§ 6 Bias-Monitoring

(1) Der Arbeitgeber führt [jährlich / halbjährlich — Streitpunkt] Bias-Tests durch. (2) Werden Bias-Probleme festgestellt, ist das System sofort anzupassen oder vorübergehend außer Betrieb zu nehmen. (3) Der Betriebsrat erhält Zugang zu aggregierten Statistiken.

§ 7 Schulung und AI Literacy

(1) Beschäftigte, die KI-Systeme nutzen, werden vor Einsatz entsprechend geschult (Art. 4 KI-VO). (2) Der Betriebsrat und seine Mitglieder erhalten eine eigene Schulung zu KI-Mitbestimmung auf Kosten des Arbeitgebers.

§ 8 Laufzeit und Kündigung

Diese Betriebsvereinbarung gilt auf unbestimmte Zeit. Sie kann von jeder Seite mit einer Frist von sechs Monaten schriftlich gekündigt werden. Bei Kündigung gilt eine Nachwirkung bis zum Abschluss einer neuen Vereinbarung.

Unterschriften

[Unterschriften nach Einigung — noch ausstehend]

ENTWURF — NICHT UNTERZEICHNET — Verhandlungsstand 08. April 2026

Aktenzeichen: TI-KI-2026-009

Mannheim, _____	Mannheim, _____
Annegret Kühnhausen CCO Thalheim Industries SE	Norbert Schäpers Betriebsratsvorsitzender Thalheim Industries SE

Datei: richtlinie-ki-einsatz-thalheim-v3-2.docx

INTERNE RICHTLINIE

Inhaltsverzeichnis

1. Zweck und Anwendungsbereich
2. Begriffsbestimmungen
3. Grundsätze
4. KI-Freigabeprozess
5. Pflichten für Hochrisiko-KI-Systeme
6. Verbotene KI-Praktiken
7. AI Literacy und Schulung
8. Datenschutz und DPIA
9. Mitbestimmung
10. Verstöße und Sanktionen
11. Inkrafttreten

1. Zweck und Anwendungsbereich

Diese Richtlinie legt konzernweit verbindliche Anforderungen für Einführung, Betrieb und Überwachung von KI-Systemen bei der Thalheim Industries SE fest. Sie dient der Umsetzung der gesetzlichen Anforderungen der Verordnung (EU) 2024/1689 (KI-Verordnung, KI-VO) sowie der DSGVO.

Die Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter, Führungskräfte und externen Auftragnehmer, die im Auftrag oder für Zwecke der Thalheim Industries SE KI-Systeme einsetzen oder entwickeln.

2. Begriffsbestimmungen

KI-System: Software, die für eine Reihe von Zielen betrieben wird und auf der Basis von Eingaben Ergebnisse wie Vorhersagen, Empfehlungen, Entscheidungen oder Inhalte erzeugt, die reale oder virtuelle Umgebungen beeinflussen (Art. 3 Nr. 1 KI-VO).

Hochrisiko-KI-System: KI-Systeme nach Art. 6 i.V.m. Anhang III KI-VO, insbesondere in den Bereichen Personalauswahl, Kreditwürdigkeitsbewertung, biometrische Identifikation und kritische Infrastruktur.

Betreiber (Deployer): Natürliche oder juristische Person, die ein KI-System in eigener Verantwortung verwendet (Art. 3 Nr. 4 KI-VO). Thalheim Industries SE ist Betreiber aller fünf Kernsysteme.

GPAI-Modell: Allzweck-KI-Modell (General-Purpose AI), das für eine Vielzahl von Aufgaben trainiert wurde und als Grundlage für andere KI-Systeme verwendet werden kann (Art. 3 Nr. 63 KI-VO). Beispiel: OpenAI GPT-4o.

Schatten-KI: Nicht gemeldete, nicht freigegebene KI-Systeme, die von Mitarbeitenden ohne Kenntnis der Compliance-Abteilung eingesetzt werden.

3. Grundsätze

1. **Rechtmäßigkeit:** KI-Systeme werden nur eingesetzt, wenn sie die anwendbaren Rechtsvorschriften erfüllen.
2. **Menschliche Aufsicht:** Keine abschließenden Entscheidungen mit wesentlichen Folgen für Personen ohne menschliche Überprüfungsmöglichkeit (Art. 14 KI-VO).

3. Transparenz: Offenlegung des KI-Einsatzes gegenüber Betroffenen; Einhaltung Art. 50 KI-VO.
4. Nicht-Diskriminierung: Regelmäßige Bias-Tests; keine systematische Diskriminierung.
5. Datenschutz by Design: DPIA vor Einsatz neuer Hochrisiko-Systeme; DSB frühzeitig einbinden.
6. Rechenschaftspflicht: Vorstand trägt Gesamtverantwortung (§ 93 AktG).

4. KI-Freigabeprozess

Jede Einführung eines neuen KI-Systems sowie jede wesentliche Änderung eines bestehenden Systems erfordert eine Freigabe durch den KI-Komitee-Vorsitz (in Abstimmung mit CDO und CCO). Der Freigabeprozess umfasst mindestens:

Meldung des geplanten Systems durch den antragstellenden Fachbereich

Risikoklassifikation nach dem Vier-Stufen-Schema (Art. 5, Art. 6 / Anh. III, Art. 50, minimal)

Datenschutzvorabprüfung durch die Datenschutzbeauftragte

Bei Hochrisiko: vollständige Konformitätsprüfung vor Inbetriebnahme

Eintrag im zentralen KI-Inventar

Nachweis AI-Literacy-Schulung des antragstellenden Fachbereichs

Die Verwendung von KI-Systemen außerhalb dieses Freigabeprozesses (Schatten-KI) ist ausdrücklich untersagt und kann disziplinarische Konsequenzen haben.

5. Pflichten für Hochrisiko-KI-Systeme

Für Hochrisiko-KI-Systeme (Art. 6 i.V.m. Anhang III KI-VO) gelten kumulativ die Pflichten nach Art. 9–17 KI-VO. Betreiber (Deployer) müssen nach Art. 26 KI-VO insbesondere:

Nur Systeme einsetzen, für die der Anbieter eine Konformitätserklärung ausgestellt hat

Die Zweckbestimmung des Systems einhalten

Menschliche Aufsicht sicherstellen (Art. 14 KI-VO)

Protokollierungsfunktionen aktiviert lassen (Art. 12 KI-VO)

Betroffene Personen informieren (Art. 13, Art. 50 KI-VO)

Schwerwiegende Vorfälle melden (Art. 73 KI-VO)

Registrierung in EU-Datenbank vornehmen (Art. 49 KI-VO)

6. Verbotene KI-Praktiken

Die Verbote des Art. 5 KI-VO gelten bei Thalheim Industries SE absolut. Insbesondere verboten sind: unterschwellige Beeinflussung, Ausnutzung von Vulnerabilitäten, Social Scoring, Emotionserkennung am Arbeitsplatz sowie biometrische Massenüberwachung. Vollständige Rote Liste: Aktenstück 09 (TI-KI-2026-013).

7. AI Literacy und Schulung (Art. 4 KI-VO)

Alle Mitarbeitenden, die KI-Systeme einsetzen oder beaufsichtigen, müssen über ausreichende KI-Kompetenz verfügen. Das Schulungsprogramm (AI-Literacy-Curriculum, Aktenstück 05) ist verbindlich zu absolvieren. Nachweise werden im LMS TalentHub geführt.

8. Datenschutz und DPIA

Für KI-Systeme, die personenbezogene Daten verarbeiten, ist eine Datenschutzvorabprüfung durchzuführen. Hochrisiko-Systeme mit Personenbezug erfordern eine vollständige Datenschutz-Folgenabschätzung (DPIA) nach Art. 35 DSGVO. Die Datenschutzbeauftragte Dr. Eichenmüller ist frühzeitig einzubeziehen.

9. Mitbestimmung

KI-Systeme, die zur Überwachung oder Leistungsbewertung von Mitarbeitenden geeignet sind, unterliegen der Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG. Diese Systeme dürfen erst nach Abschluss einer Betriebsvereinbarung oder durch Entscheidung der Einigungsstelle in Betrieb genommen werden.

10. Verstöße und Sanktionen

Verstöße gegen diese Richtlinie — insbesondere der Einsatz von Schatten-KI oder die Umgehung des Freigabeprozesses — werden als Pflichtverletzung gewertet und können arbeitsrechtliche Konsequenzen bis hin zur Kündigung nach sich ziehen. Schwere Verstöße mit Behördenrelevanz werden durch die CCO der zuständigen Aufsichtsbehörde gemeldet.

11. Inkrafttreten

Diese Richtlinie tritt nach Freigabe durch den Vorstand (geplant 15. April 2026) in Kraft und löst Richtlinie KI-Einsatz v3.1 (Oktober 2025) ab. Sie wird jährlich und bei wesentlichen Änderungen der Rechtslage anlassbezogen überprüft.

Mannheim, Februar 2026
Annegret Kühnhausen Dr. Falk Roosendaal
Chief Compliance Officer KI-Komitee-Vorsitz

Dokumentnummer	TI-RICHTLINIE-KI-2026-001
Version	3.2 (Entwurf, Vorstandsfreigabe ausstehend)
Erstellt	Dr. F. Roosendaal / A. Kühnhausen
Geprüft	Kanzlei Borchmann Compliance
Geltungsbereich	Thalheim Industries SE + alle EU-Tochtergesellschaften
Ablöst	Richtlinie KI-Einsatz v3.1 (Oktober 2025)
Nächste Überprüfung	Februar 2027

Datei: vorstandsvorlage-ki-governance-rahmen.docx

VORSTANDSVORLAGE
KI-Governance-Rahmen Thalheim Industries SE

1. Ausgangslage und Handlungsbedarf

Die Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-VO) tritt mit gestaffelten Anwendungsfristen in Kraft. Für Hochrisiko-KI-Systeme nach Art. 6 i.V.m. Anhang III KI-VO gilt die vollständige Anwendungsfrist ab 02. August 2026. Thalheim Industries SE betreibt derzeit zwei Hochrisiko-Systeme (RecruitAI, CreditVision Score) sowie drei weitere KI-Systeme mit

Compliance-Relevanz.

Ohne ein strukturiertes KI-Governance-Programm drohen folgende Konsequenzen: • Bußgelder nach Art. 99 KI-VO bis zu 15 Mio. EUR (Hochrisiko-Pflichtverletzungen) • Persönliche Haftung der Vorstandsmitglieder nach § 93 AktG • Behördliche Einschränkung oder Untersagung des Systembetriebs • Reputationsschäden gegenüber Kunden, Investoren und Betriebsrat

2. Beschlussgegenstand

Der Vorstand wird gebeten, folgende Beschlüsse zu fassen:

Einrichtung des Programms TI-KI-2026 (Laufzeit Oktober 2025 – Dezember 2027)

Ernennung von Dr. Falk Roosendaal zum KI-Komitee-Vorsitz

Mandatierung der Kanzlei Borchmann Compliance (Frankfurt) als externe Rechtsberatung

Mandatierung der WPG Hagedorn & Partner als externer Auditor für Konformitätsbewertungen

Genehmigung eines Programm-Gesamtbudgets von 1.450.000 EUR für Phase 1 und 2

Beauftragung der CCO, unverzüglich Betriebsvereinbarungsverhandlungen mit dem Betriebsrat aufzunehmen

3. KI-Systeme im Scope

4. Programm-Struktur und Meilensteine

Phase 1 (Oktober–Dezember 2025): Inventarisierung und Gap-Analyse

Vollständige Erfassung aller KI-Systeme, Risikoklassifikation nach KI-VO, Identifikation Compliance-Lücken.

Phase 2 (Januar–Juli 2026): Konformitätsherstellung

Konformitätsprüfung Hochrisiko-Systeme, DPIA, Betriebsvereinbarung, AI-Literacy-Schulung, Vendor-Vertragsnachträge, Behördenkommunikation (BaFin, LfDI BW).

Phase 3 (Januar–Dezember 2027): Konsolidierung

Jährliche Bias-Tests, Governance-Optimierung, Audit-Readiness, Überprüfung neuer Systeme.

5. Rechtliche Grundlagen

• Verordnung (EU) 2024/1689 (KI-VO), insbesondere Art. 4, 6, 9–17, 43, 50, 73, 99, 113 • DSGVO (EU) 2016/679, insbesondere Art. 22, 35 • BetrVG § 87 Abs. 1 Nr. 6 (Mitbestimmung technische Überwachungseinrichtungen) • AktG § 93 (Vorstandshaftung und Sorgfaltspflicht) • Hinweisgeberschutzgesetz (HinSchG)

6. Empfehlung

CCO und CIO empfehlen dem Vorstand einstimmig, alle unter Abschnitt 2 aufgeführten Beschlüsse zu fassen. Der Handlungsbedarf ist dringend — die Anwendungsfristen der KI-VO lassen keinen Aufschub.

Mannheim, 15. Oktober 2025

Dr. Sigrid Wolfsbacher Annegret Kühnhausen

Chief Information Officer Chief Compliance Officer

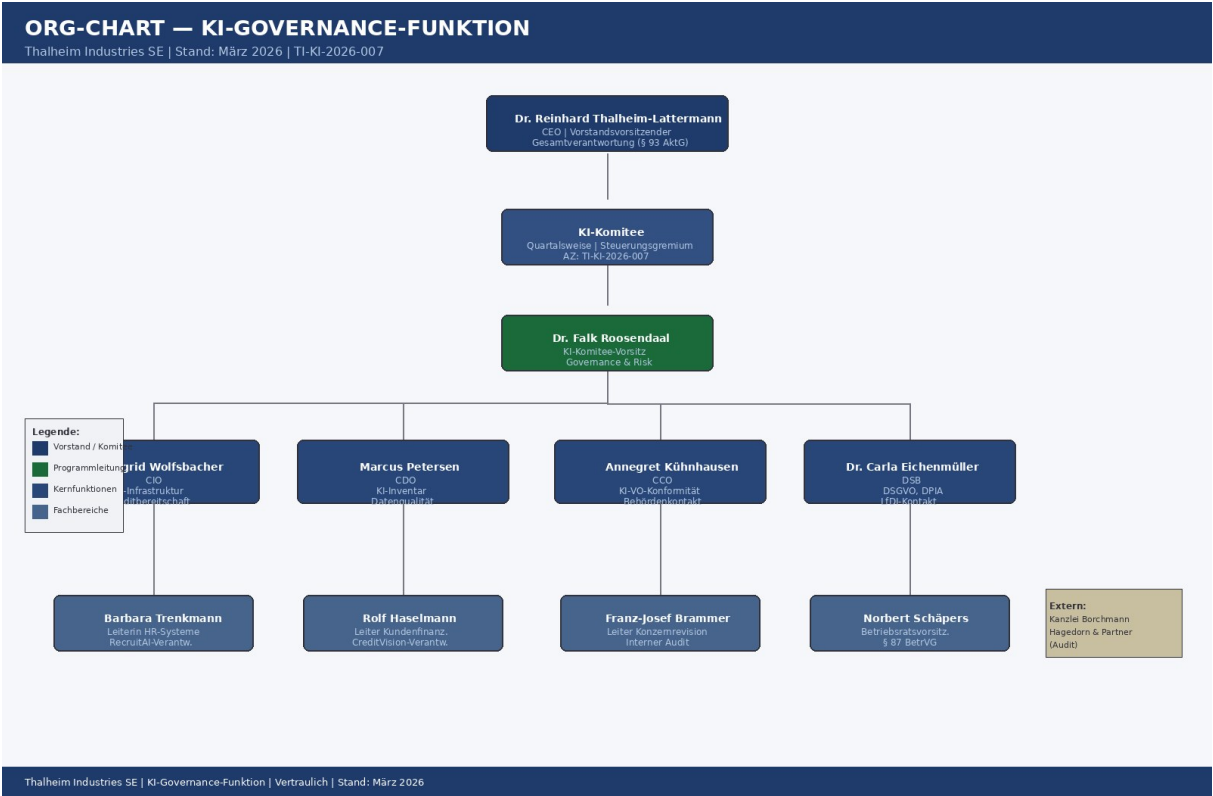
Thalheim Industries SE Thalheim Industries SE

Aktenzeichen	TI-KI-2026-007
Datum	15. Oktober 2025
Vorgelegt durch	CIO Dr. Wolfsbacher; CCO Kühnhausen
Beschlusnummer	VS-2025-087
Klassifizierung	VERTRAULICH — Nur Vorstandsmitglieder
Entscheidungsbedarf	Ja — Programm TI-KI-2026 zu beschließen

System	Einsatzbereich	Risikoklasse	Vendor	Frist
RecruitAI	HR / Recruiting	Hochrisiko (Anh. III Nr. 4a)	Synaptec Analytics GmbH	02.08.2026
CreditVision Score	Kundenfinanzierung	Hochrisiko (Anh. III Nr. 5b)	CreditVision AG	02.08.2026
PredictMaint	Predictive Maintenance	Begrenztes Risiko	Intern	02.08.2027
CodeAssist	Software-Entwicklung	Begrenztes Risiko (GPAI)	OpenAI Ireland	02.08.2027
ServiceBot	Kundenservice	Transparenzpflichten (Art. 50)	Intern	02.02.2025 ✓

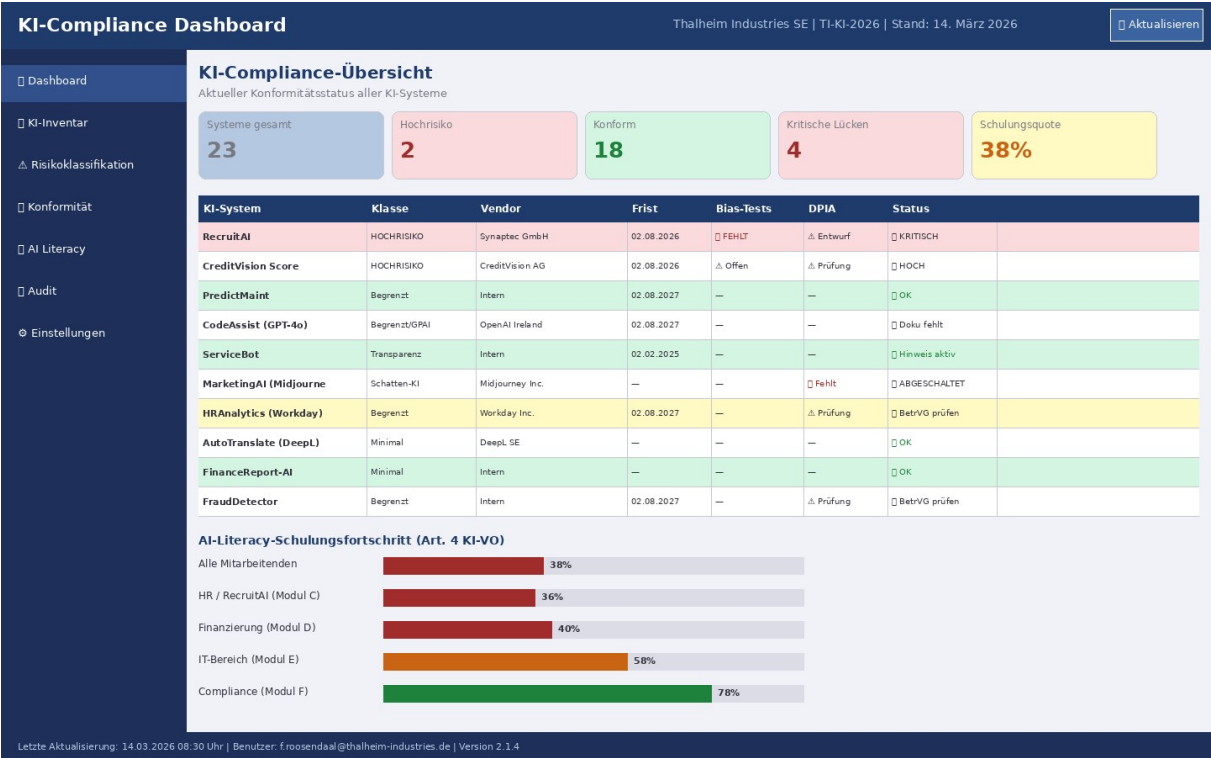
Bildanlagen und Screenshots

Datei: org-chart-governance-funktion.jpg



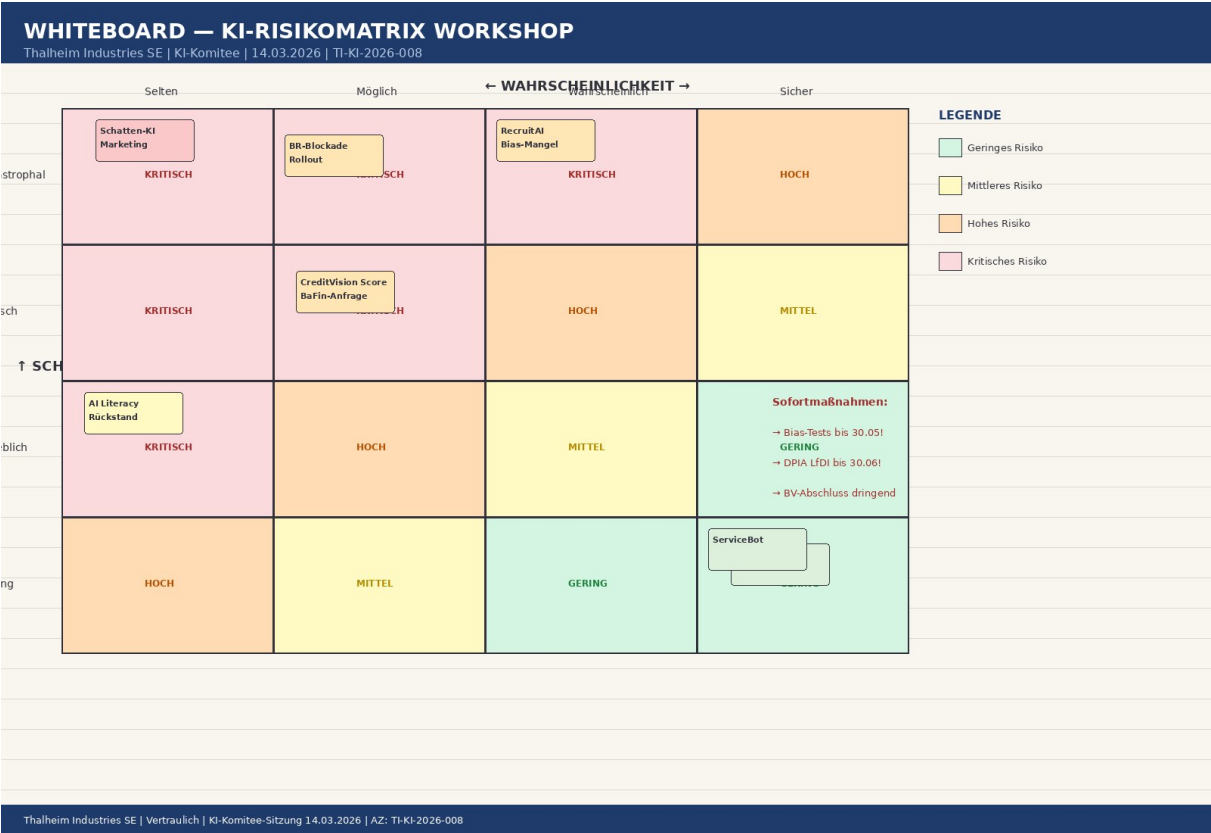
Bilddatei: org-chart-governance-funktion.jpg

Datei: screenshot-dashboard-konformitaet.jpg



Bilddatei: screenshot-dashboard-konformitaet.jpg

Datei: whiteboard-risikomatrix.jpg



Bilddatei: whiteboard-risikomatrix.jpg

PDF-Anhang: eu-leitlinien-zusammenfassung.pdf

Datei: eu-leitlinien-zusammenfassung.pdf

EU-Leitlinien zur KI-Verordnung

Zusammenfassung wesentlicher Anforderungen für die Praxis

Verordnung (EU) 2024/1689 | Stand: März 2026 | Aktenzeichen: TI-KI-2026-007
Erstellt für: KI-Komitee Thalheim Industries SE | Kanzlei Borchmann Compliance, Frankfurt

1. Einleitung: Warum die KI-Verordnung?

Die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über künstliche Intelligenz (KI-VO) ist das erste umfassende gesetzliche Regelwerk der Welt für KI-Systeme. Sie verfolgt einen risikobasierten Ansatz: Je höher die Risiken eines KI-Systems für Grundrechte, Sicherheit oder Gesundheit, desto strenger die Anforderungen.

Die KI-VO gilt für alle Unternehmen, die KI-Systeme in der EU in Verkehr bringen, in Betrieb nehmen oder nutzen — unabhängig vom Unternehmenssitz. Thalheim Industries SE ist als Betreiber (Deployer) im Sinne von Art. 3 Nr. 4 KI-VO von den Betreiberpflichten betroffen.

2. Anwendungsfristen (Art. 113 KI-VO)

Die KI-VO tritt mit gestaffelten Fristen in Kraft. Quelle: <https://dejure.org/gesetze/KIVO/113.html>

Datum	Anwendbare Regelungen
02.02.2025	Art. 5 (Verbote), Art. 50 (Transparenzpflichten)
02.08.2025	Kapitel I, II (Allg. Bestimmungen), Art. 4 (AI Literacy), Kap. III Titel 1-2 (Governance)
02.08.2026	Art. 6-51 (Hochrisiko-Pflichten, Konformitätsbewertung, Registrierung, GPAI-Pflichten)
02.08.2027	Art. 6 für bestehende Hochrisiko-Produkte nach Anhang I (CE-Kennzeichnung)

3. Das Risikoschema der KI-VO

Die KI-VO ordnet KI-Systeme nach einem Vierstufenmodell:

Risikoklasse	Grundlage	Anforderungen	Beispiele
Unannehmbares Risiko (VERBOTEN)	Art. 5 KI-VO	Absolutes Verbot des Einsatzes	Social Scoring, Emotionserkennung Arbeitsplätze
Hochrisiko	Art. 6, Anh. III KI-VO	Vollständige Pflichten Art. 9-17; Konformitätsbewertung; Registrierung	Perfekte Bewerber-Identifizierung, Identifizierung
Begrenztes Risiko / GPAI	Art. 50, Art. 51 ff. KI-VO	Transparenzpflichten; GPAI-Modelldokumentation	Generative AI-Tools, Bildgeneratoren
Minimales Risiko	—	Keine spezifischen KI-VO-Pflichten	Spam-Filter, Rechtschreibkorrektur

4. Wesentliche Hochrisiko-Pflichten (Art. 9–17 KI-VO)

Art. 9 — Risikomanagementsystem

Laufendes Risikomanagementsystem; identifiziert bekannte und vorhersehbare Risiken, Bias-Tests nach Art. 9 Abs. 7. URL: <https://dejure.org/gesetze/KIVO/9.html>

Art. 10 — Daten-Governance

Trainings-, Validierungs- und Testdaten müssen relevant, repräsentativ, fehlerfrei und vollständig sein.

Art. 11 — Technische Dokumentation

Vollständige Dokumentation nach Anhang IV KI-VO; vor Inbetriebnahme zu erstellen; Behörden zugänglich zu machen.

Art. 12 — Protokollierung

Automatische Protokollierung von Ereignissen über die Lebensdauer des Systems.

Art. 13 — Transparenz

Betreiber erhalten eine Gebrauchsanweisung; Transparenz gegenüber betroffenen Personen.

Art. 14 — Menschliche Aufsicht

Technische und organisatorische Maßnahmen zur menschlichen Aufsicht; Override-Möglichkeit; kein vollständiger Automatismus.

Art. 15 — Genauigkeit, Robustheit, Cybersicherheit

Nachgewiesene Leistungsfähigkeit; Adversarial-Robustheit; Cybersicherheitsstandards.

Art. 26 — Betreiberpflichten (Deployer)

Nur konforme Systeme nutzen; Zweckbestimmung einhalten; Meldepflichten; Protokolle 6 Monate aufbewahren. URL: <https://dejure.org/gesetze/KIVO/26.html>

Art. 43 — Konformitätsbewertung

Interne Konformitätsbewertung (für Systeme in Anh. III Nr. 1-7) oder Drittprüfung (biometrische Systeme); vor Inbetriebnahme abzuschließen.

Art. 49 — Registrierung EU-Datenbank

Hochrisiko-Systeme sind vor Inbetriebnahme in der EU-KI-Datenbank zu registrieren.

5. AI Literacy (Art. 4 KI-VO)

Anbieter und Betreiber müssen sicherstellen, dass ihr Personal und alle Personen, die im Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ausreichende KI-Kompetenz verfügen. Art. 4 KI-VO gilt seit 02.08.2025. URL: <https://dejure.org/gesetze/KIVO/4.html>

Kriterien für ausreichende KI-Kompetenz: technische Kenntnisse; Erfahrung; Ausbildung und Schulung; Kontext des KI-System-Einsatzes. Die Anforderungen sind kontextabhängig — ein einfacher Nutzer eines Chatbots braucht weniger Wissen als ein HR-Business-Partner, der RecruitAI-Ergebnisse bewertet.

6. Verbotene Praktiken (Art. 5 KI-VO)

Seit 02.02.2025 gelten folgende Verbote absolut (Art. 5 KI-VO, <https://dejure.org/gesetze/KIVO/5.html>):

- Unterschwellige Beeinflussung ohne Wissen der betroffenen Person mit Schadensabsicht oder -wirkung
- Ausnutzung von Vulnerabilitäten (Alter, Behinderung, wirtschaftliche Lage)
- Social Scoring durch öffentliche Stellen oder vergleichbare private Akteure

- Biometrische Echtzeit-Fernidentifikation in öffentlichen Räumen (durch Strafverfolgungsbehörden)
- Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen (außer medizinischen/Sicherheitsgründen)
- Biometrische Kategorisierung nach politischen Ansichten, Religion, Gewerkschaftszugehörigkeit, Sexualleben
- Predictive Policing: Kriminalitätsrisiko-Einstufung nur auf Basis von Persönlichkeitsmerkmalen
- Anlasslose biometrische Massenüberwachung öffentlicher Räume

7. Schnittstellen zur DSGVO

Die KI-VO und die DSGVO gelten nebeneinander. Wesentliche Berührungspunkte:

Art. 22 DSGVO — Automatisierte Einzelentscheidungen

Recht auf Nichtunterwerfung unter automatisierte Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung; Widerspruchsrecht; Erklärungsrecht. URL: <https://dejure.org/gesetze/DSGVO/22.html>

Art. 35 DSGVO — DPIA

Für KI-Systeme, die systematisch persönliche Aspekte bewerten (z. B. Scoring), ist eine DPIA erforderlich. Koordination mit Art. 9 KI-VO-Risikomanagement empfohlen. URL: <https://dejure.org/gesetze/DSGVO/35.html>

Art. 28 DSGVO — Auftragsverarbeitung

Vendor-Verträge müssen DSGVO-konforme AVV enthalten. KI-VO-Anforderungen (Bias-Tests, Doku) sollten als zusätzliche Klauseln ergänzt werden.

PDF-Anhang: gutachten-externer-kanzlei-ki-vo-anwendung.pdf

Datei: gutachten-externer-kanzlei-ki-vo-anwendung.pdf

RECHTSGUTACHTEN

Anwendung der Verordnung (EU) 2024/1689 (KI-Verordnung) auf die KI-Systeme der Thalheim Industries SE

Auftraggeber:	Thalheim Industries SE, August-Bebel-Ring 14, 68163 Mannheim
Datum:	15. Februar 2026
Verfasserin:	Dr. Nora Borchmann, LL.M. (LSE), Rechtsanwältin
Aktenzeichen:	TI-KI-2026-007 (Thalheim); BC-KI-2026-0112 (Kanzlei)
Vertraulichkeit:	VERTRAULICH — Anwaltliches Mandatsverhältnis

Executive Summary

Die Kanzlei Borchmann Compliance wurde von der Thalheim Industries SE beauftragt, die Anwendbarkeit der Verordnung (EU) 2024/1689 (KI-VO) auf die fünf KI-Kernsysteme des Unternehmens zu prüfen und eine Handlungsempfehlung für das KI-Governance-Programm TI-KI-2026 zu erstellen.

Kernaussagen dieses Gutachtens:

- RecruitAI (Synaptec Analytics GmbH) ist eindeutig als Hochrisiko-System nach Art. 6 Abs. 2 i.V.m. Anhang III Nr. 4 lit. a KI-VO einzustufen. Die Konformitätspflichten sind vollständig und fristgerecht bis 02.08.2026 zu erfüllen.
- CreditVision Score ist Hochrisiko nach Art. 6 Abs. 2 i.V.m. Anhang III Nr. 5 lit. b KI-VO. Art. 22 DSGVO und KI-VO-Anforderungen stehen in kumulativer Anwendung.
- Der Betrieb von KI-Systemen ohne Betriebsvereinbarung nach § 87 Abs. 1 Nr. 6 BetrVG ist mit erheblichen arbeitsrechtlichen Risiken verbunden.
- Die Schatten-KI in der Marketingabteilung (Midjourney) stellt einen potenziellen Verstoß gegen Art. 44 ff. DSGVO (Drittlandübermittlung) dar.
- Die fehlende flächendeckende AI-Literacy-Schulung nach Art. 4 KI-VO begründet eine aktuelle Compliance-Lücke seit August 2025.

I. Rechtlicher Rahmen

Die KI-VO ist eine unmittelbar anwendbare Verordnung des Europäischen Parlaments und des Rates. Sie entfaltet unmittelbare Wirkung in allen EU-Mitgliedstaaten und bedarf keiner nationalen Umsetzung. Deutschland hat die KI-VO als unmittelbar anwendbares Recht; zuständige Marktüberwachungsbehörde ist in Deutschland die Bundesnetzagentur.

Einschlägige Vorschriften (mit Quellenangaben):

- KI-VO Art. 4 (AI Literacy): <https://dejure.org/gesetze/KIVO/4.html>
- KI-VO Art. 5 (Verbote): <https://dejure.org/gesetze/KIVO/5.html>
- KI-VO Art. 6 und Anhang III (Hochrisiko): <https://dejure.org/gesetze/KIVO/6.html>
- KI-VO Art. 9-17 (Hochrisiko-Pflichten): <https://dejure.org/gesetze/KIVO/9.html>

- KI-VO Art. 26 (Betreiberpflichten): <https://dejure.org/gesetze/KIVO/26.html>
- KI-VO Art. 50 (Transparenzpflichten): <https://dejure.org/gesetze/KIVO/50.html>
- KI-VO Art. 113 (Anwendungsfristen): <https://dejure.org/gesetze/KIVO/113.html>
- DSGVO Art. 22 (Automatisierte Einzelentscheidung): <https://dejure.org/gesetze/DSGVO/22.html>
- DSGVO Art. 35 (DPIA): <https://dejure.org/gesetze/DSGVO/35.html>
- BetrVG § 87 (Mitbestimmung): <https://dejure.org/gesetze/BetrVG/87.html>
- AktG § 93 (Vorstandshaftung): <https://dejure.org/gesetze/AktG/93.html>

II. Klassifikation der KI-Systeme

Die Kanzlei hat alle fünf Kernsysteme einer umfassenden Klassifikationsprüfung unterzogen. Die Ergebnisse entsprechen der internen Klassifikation durch das KI-Komitee (Aktenstück 02, TI-KI-2026-008) und werden von der Kanzlei bestätigt und juristisch untermauert.

II.1 RecruitAI — Rechtliche Einordnung als Hochrisiko

RecruitAI unterstützt Entscheidungen über die Einstellung, Ablehnung und Priorisierung von Bewerberinnen und Bewerbern. Dies fällt klar unter Anhang III Nr. 4 lit. a KI-VO: 'KI-Systeme, die für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern, Bewerber zu bewerten und zu priorisieren.'

Die Hochrisiko-Einstufung ist unzweifelhaft. Thalheim Industries SE hat als Betreiber sämtliche Pflichten nach Art. 9-17 i.V.m. Art. 26 KI-VO zu erfüllen. Besonderes Augenmerk gilt Art. 9 Abs. 7 KI-VO (Bias-Tests), da der Auditor Hagedorn & Partner hier einen kritischen Mangel festgestellt hat.

Rechtliche Bewertung des Mangels Bias-Tests: Das Fehlen von Bias-Tests stellt eine unmittelbare Gefährdung der Anforderung nach Art. 9 Abs. 7 KI-VO dar. Es erhöht zudem das Risiko einer Verletzung von Art. 21 GrCh (Nichtdiskriminierung) erheblich. Die Kanzlei empfiehlt, eigene Bias-Tests unverzüglich zu beauftragen und Synaptec zur Vertragserfüllung aufzufordern. Sollte Synaptec bis 30.05.2026 keine Tests vorgelegt haben, empfehlen wir eine Abmahnung nach § 323 BGB als erste Stufe der Vertragsdurchsetzung.

II.2 CreditVision Score — Art. 22 DSGVO und KI-VO

CreditVision Score berechnet Bonitätsscores für Privat- und Gewerbekunden. Die Einstufung als Hochrisiko nach Anhang III Nr. 5 lit. b KI-VO ('KI-Systeme zur Bewertung der Kreditwürdigkeit natürlicher Personen oder zur Feststellung ihrer Kreditwürdigkeit') ist eindeutig.

Zur BaFin-Anfrage (GZ BJ 24-K 7102-2026/0012): Die BaFin fragt nach Art. 22 DSGVO-Konformität und der Konformitätsbewertung nach Art. 43 KI-VO. Empfehlung der Kanzlei für die Stellungnahme: Darlegen, dass (1) ein Mensch die abschließende Kreditentscheidung trifft, (2) Informationspflichten nach Art. 13 DSGVO implementiert sind, (3) Widerspruchsrecht nach Art. 22 Abs. 3 DSGVO im Kundenprozess verankert ist. Die Konformitätsbewertung sollte als 'in Bearbeitung, Abschluss 31.07.2026' angekündigt werden.

Relevante Rechtsprechung: EuGH, Urteil vom 07.12.2023, Rs. C-634/21 (SCHUFA Holding AG / WIBV). Der EuGH hat klargestellt, dass die Übermittlung eines Scorewerts durch eine Auskunft an einen Verantwortlichen unter Art. 22 DSGVO fallen kann, wenn der Verantwortliche den Score praktisch determinierend zugrunde legt. Gleiches gilt für Thalheim, wenn CreditVision Score faktisch determinierend wirkt (94 % Folgebereitschaft der Sachbearbeiter).

III. Betriebsratsrecht (§ 87 BetrVG)

Der Betriebsrat hat ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG bei Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind oder geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. URL: <https://dejure.org/gesetze/BetrVG/87.html>

Einschlägige Rechtsprechung: BAG, Beschluss vom 13.12.2022 (1 ABR 28/21): KI-gestützte Systeme, die Leistungsdaten von Beschäftigten auswerten, auch wenn nicht primär zu Überwachungszwecken konzipiert, können § 87 Abs. 1 Nr. 6 BetrVG unterfallen, wenn sie zur Leistungsüberwachung geeignet sind. Die Kanzlei empfiehlt, nicht auf die 'Primärfunktion' zu abstellen, sondern auf die objektive Eignung zur Überwachung.

Folge für Thalheim: RecruitAI ist objektiv geeignet, Leistungs- und Qualifikationsdaten von Beschäftigten zu verarbeiten. Das Mitbestimmungsrecht des BR ist daher zu bejahen. Ein Betrieb ohne Betriebsvereinbarung oder Einigungsstellenspruch ist rechtswidrig und kann durch einstweilige Verfügung untersagt werden.

IV. Haftungsrisiken Vorstand (§ 93 AktG)

§ 93 Abs. 1 AktG (<https://dejure.org/gesetze/AktG/93.html>) verpflichtet Vorstandsmitglieder zur Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters. Die Nichtimplementierung der KI-VO-Anforderungen bei bekannten Hochrisiko-Systemen stellt nach Auffassung der Kanzlei eine Sorgfaltspflichtverletzung dar, wenn der Vorstand die Risiken kennt oder kennen muss (was nach Vorstandsbeschluss VS-2025-087 zu bejahen ist) und keine angemessenen Gegenmaßnahmen ergreift.

Die Kanzlei empfiehlt dem Vorstand daher: regelmäßige dokumentierte Befassung mit dem Programmfortschritt; unverzügliche Eskalation bei Rückständen; aktive Entscheidung bei Synaptec-Eskalation, Betriebsvereinbarung und DSGVO-Meldepflicht (vgl. Eskalationsvorlage Aktenstück 17).

V. Gesamtbewertung und Handlungsempfehlungen

Die Kanzlei Borchmann Compliance bewertet den Gesamtstand der KI-Compliance bei Thalheim Industries SE per März 2026 als kritisch, aber steuerbar. Die strukturelle Governance ist gut aufgestellt. Die kritischen Risiken (Bias-Tests, Betriebsvereinbarung, AI Literacy, DPIA) sind identifiziert und in Bearbeitung.

1. Synaptec-Vertragsdurchsetzung: Unverzüglich formelle Mängelrüge nach § 634 BGB; parallele eigene Bias-Tests.
2. Betriebsvereinbarung: Aktive Verhandlungsstrategie; wenn keine Einigung bis 15.05.2026, Einigungsstelle nach § 76 BetrVG anrufen.
3. AI Literacy: Sofortprogramm mit Führungskräftepflicht; monatliches Reporting.
4. DPIA RecruitAI: Bearbeitung priorisieren; LfDI-Frist 30.06.2026 einhalten.
5. BaFin-Stellungnahme: Vollständig und fristgerecht (15.05.2026) beantworten.
6. Vendor-Verträge: KI-VO-Klauseln in alle Vendor-Verträge bis 30.06.2026 einbauen.
7. Schatten-KI: DSGVO-Meldepflicht prüfen; technische Prävention implementieren.

Dokument ist ein anwaltliches Mandatsdokument und unterliegt dem anwaltlichen Verschwiegenheitsgebot.