

## RECHTSGUTACHTEN

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

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