

KI - UNTERSTÜTZUNG ODER GEFAHR FÜR DIE INFORMATIONSSICHERHEIT?

19.02.2026

AGENDA

- 1 Kurzvorstellung migosens GmbH
- 2 Was ist Künstliche Intelligenz?
- 3 Risiken aus Sicht der Informationssicherheit
- 4 Nutzen von KI
- 5 Sicherer Einsatz von KI aus Compliance-Sicht





Stephan Auge

Teamleiter Managementsysteme
migosens GmbH
Mülheim an der Ruhr

- > ISMS Lead Auditor ISO/IEC 27001 i.A.d. TÜV Rheinland
- > Kritis-Prüfer gem. §8a BSIG
- > Prüfer „Systeme zur Angriffserkennung“ gem. BSIG
- > QMS Lead Auditor ISO 9001 i.A.d. TÜV Rheinland
- > langjährige Erfahrung im Bereich integrierte Managementsysteme

Wir sind Ihr Spezialist in den Bereichen Informationssicherheit,
Datenschutzmanagement und Work Smart



„UNSERE MITARBEITER SIND **JURISTEN, TECHNIKER, INFORMATIKER, KAUFLEUTE UND PROZESSMANAGER**. SOMIT KÖNNEN WIR ALLE ASPEKTE EINER FACHLICHEN HERAUSFORDERUNG UMFASSEND BETRACHTEN UND LÖSUNGEN MIT WEITBLICK ANBIETEN.“

Heiko Gossen, Geschäftsführer



► Unser Serviceportfolio gliedert sich in vier Bereiche

migosens



datenschutz

Strategische und operative
Beratung
Audits (intern/extern)
Datenschutzbeauftragter
branchenübergreifende
Datenschutzkonzepte
Projektbegleitung



managementssysteme*

Beratung
Audits (intern/extern)
Informationssicherheits- und
Qualitätsmanagementbeauftragter
Einführung von
Managementsystemen für
Informationssicherheit, Datenschutz,
Qualität und Business Continuity



worksmart

Führung und Zusammenarbeit
Organisationsentwicklung
Arbeitsumfeld gestalten



akademie

Datenschutzbeauftragten-
Ausbildung
Projekte und Prozesse
Informationssicherheit
Integrierte
Managementsysteme

ERFAHRUNG. WISSEN. BERATUNG.

* ein Angebot der migosens management GmbH

Was ist Künstliche Intelligenz?

„Künstliche Intelligenz ist die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren.

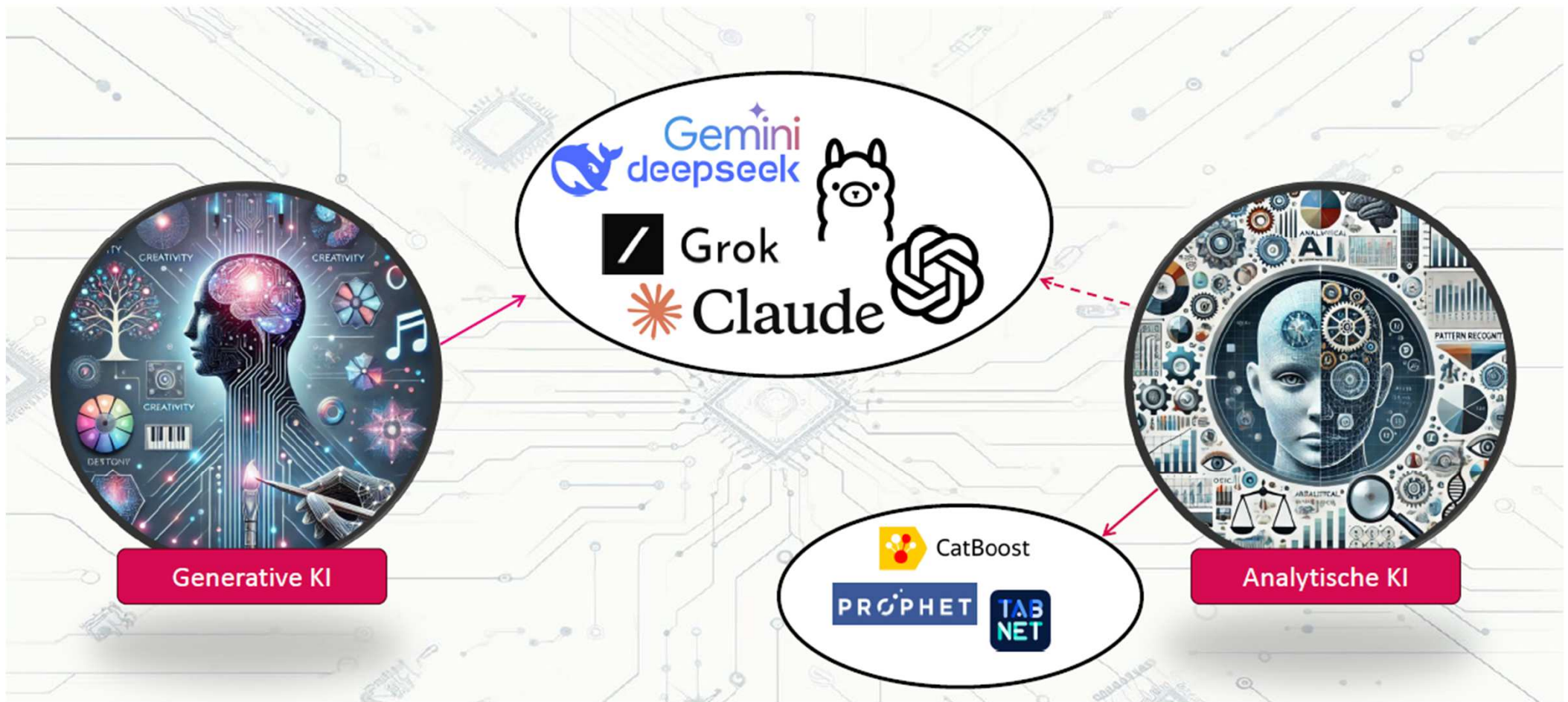
KI-Systeme sind in der Lage, ihr **Handeln anzupassen**, indem sie die Folgen früherer Aktionen analysieren und **autonom arbeiten**.“
Europäisches Parlament

Für den Zwecke der EU Verordnung (EU AI Act) gilt die Definition:

"KI-System": ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können“.

WICHTIG: Es gibt keine allgemeingültige bzw. einheitlich genutzte Definition von KI

Was ist Künstliche Intelligenz?



Was ist Künstliche Intelligenz?

HARDWARE

Massive Verbesserungen von Hardware (GPU, multicore) ermöglichen den Einsatz neuer Technologien

NETZWERKE

Daten werden in Netzwerken, Clouds sowie anderen Systemen gespeichert; die Verknüpfung von Wissen ist gegenwärtig schnell möglich

DATENVOLUMEN

Durch eine jahrzehntelange Erzeugung und Speicherung von Daten ist der Einsatz von KI erfolgreich und praxistauglich

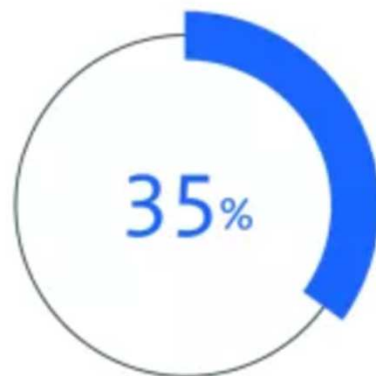


Große Datenmengen sind die Grundlage für die Nutzung von Künstlicher Intelligenz

Risiken aus Sicht der Informationssicherheit

KI gilt als neue Herausforderung für die IT-Sicherheit

Welcher der folgenden Aussagen stimmen Sie am ehesten zu?



Die Verbreitung von generativer KI wird die **IT-Sicherheit verbessern**, weil sie bei der Abwehr von Cyberangriffen genutzt werden kann.



Die Verbreitung von generativer KI wird die **IT-Sicherheit gefährden**, weil sie von Cyberangreifern genutzt werden kann.

Basis: Alle Unternehmen (n=1.002) | nicht dargestellt: »Weiß nicht/k. A.« | Quelle: Bitkom Research 2023

bitkom

Risiken aus Sicht der Informationssicherheit

- **Sicherheitslücken:** Ausnutzung von Schwachstellen in den Algorithmen, um Datenzugriff zu erlangen oder Systeme zu manipulieren
- **Bias und Diskriminierung:** Treffen von diskriminierenden Entscheidungen, wenn auf fehlerhafte Daten oder Informationen zugegriffen wird
- **Datenschutzprobleme:** Gefährdung der Privatsphäre von Nutzern
- **Automatisierung und Arbeitsplatzverlust:** Automatisierung kann zum Verlust von Arbeitsplätzen führen

Nutzen von KI

IT-Bereich

- **Predictive Maintenance:** Einsatz von KI zur Vorhersage und Vermeidung von Systemausfällen
- **Cybersecurity:** Nutzung von KI zur Erkennung und Abwehr von Cyberangriffen, Anomalieerkennung und IDS
- **Helpdesk-Automatisierung:** KI-gestützte Chatbots zur Unterstützung des IT-Supports

OT-Bereich

- **Smart Manufacturing:** Optimierung von Produktionsprozessen durch KI-gestützte Analysen
- **Energie-Management:** KI zur Überwachung und Optimierung des Energieverbrauchs in industriellen Anlagen
- **Qualitätskontrolle:** Einsatz von KI zur automatisierten Inspektion und Qualitätsprüfung von Produkten

Nutzen von KI im ISMS

- **Automatisierung von Sicherheitsprozessen:** Patchmanagement, automatisierte Reaktionen
- **Datenanalyse und Vorhersage:** Predictive Analytics, Risikobewertung
- **Verbesserung von Sicherheitsrichtlinien:** Duplikatserkennung
- **Schulung und Sensibilisierung:** Phishing-Simulationen
- **Kontinuierliche Systemüberwachung und Berichterstattung**

Sicherer Einsatz von KI aus Compliance-Sicht

Verschiedene regulatorische Regelwerke mit unterschiedlichen Anforderungen, jedoch einem Ziel:
Stärkung der digitalen Sicherheit und Resilienz

DSGVO

- Schutz der Privatsphäre und pbD von Menschen
- Informations-/Auskunfts-pflichten
- Risikomanagement (DSFA)
- VVT
- AVV
- Sicherheitskonzepte (TOM)
- Überwachung/Audits
- Schulung/Awareness
- Meldepflichten

NIS-2

- hohes gemeinsames Sicherheitsniveau in bestimmten Sektoren
- ISMS
- Risikomanagement
- Sicherheitskonzepte (TOM)
- Lieferantenmanagement
- Überwachung/Prüfung
- Schulung/Awareness
- Meldepflichten

KRITIS-DACH/CER

- physischer Schutz kritischen Infrastrukturen
- Risikomanagement
- Sicherheitskonzepte (TOM)
- Branchenstandards
- Überwachung/Prüfung
- Meldepflichten

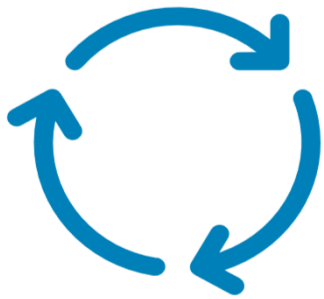
DORA-VO

- betriebliche Cyberresilienz digitaler Systeme im Finanzsektor
- Risikomanagement
 - Business Impact & Risiko Analysen
 - Notfallmanagement (BCM)
 - Access-Management oder Patchmanagement
- Lieferantenmanagement (Drittanbieter)
- Sicherheitskonzepte (TOM)
- Einführung von technischen Lösungen wie SIEM
- Überwachung/Prüfung
- Meldepflichten

KI-VO

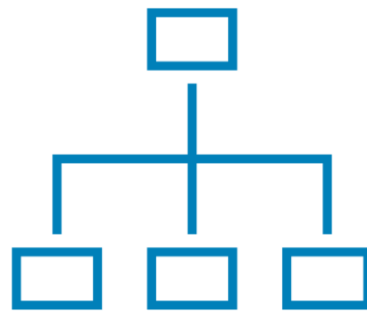
- Sicherheit und Transparenz beim Einsatz von KI
- Risikomanagement
- Transparenzpflichten
- Sicherheitskonzepte (TOM)
- Lieferantenmanagement
- Schulung/Awareness
- Meldepflichten

Anforderung an die Implementierung gem. KI-VO



Technologische Infrastruktur und Dokumentation

- Art. 11 KI-VO
- Art. 13 KI-VO
- Art. 23 Abs. 1 lit. b, c KI-VO
- Art. 26 Abs. 1 KI-VO
- Art. 53 Abs. 1 lit. a KI-VO



Datenmanagement und Transparenz

- Art. 1 KI-VO
- Art. 10 KI-VO
- Art. 13 KI-VO
- Art. 26 Abs. 6, 11 und 12 KI-VO
- Art. 53 Abs. 1 lit. a KI-VO



Schulung und Awareness sowie Informationspflichten

- Art. 4 KI-VO
- Art. 26 Abs. 2 und Abs. 7 KI-VO



Regulatorische Anforderungen

KI-VO, KI-Haftungs-RL (Entwurf), AGG, DSGVO, BDSG, BetrVG, BGB, DA, DDG, DGA, GG, GrCH, ProdHaftG, UrhG, GeschGehG, Patentrecht, [weitere normative und regulatorischen Anforderungen DORA-VO, NIS-2, CER-RL, KRITIS-Dachgesetz](#)

Bedeutung für die Informationssicherheit/ Cyberresilienz



Schutz
sensibler Daten
und Systeme

Sicherheitsmaßnahmen gem. Art. 14,15 Hochrisiko:

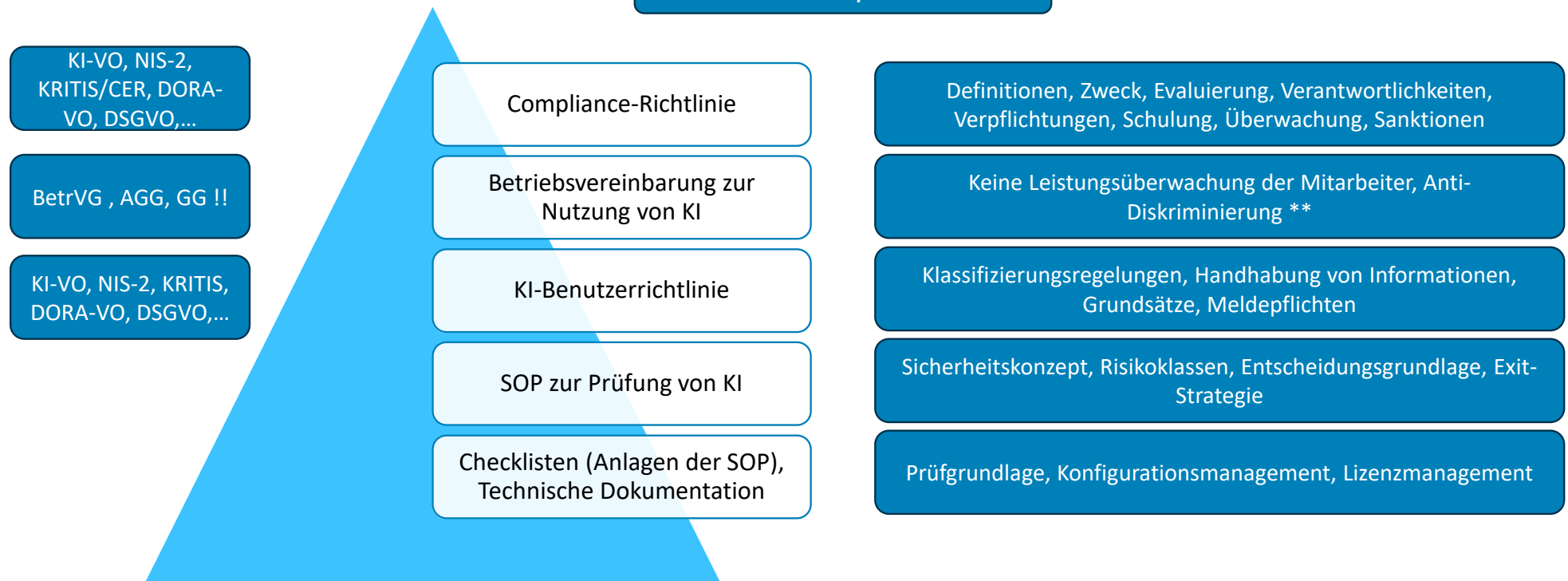
- **Zugriffskontrollen** z.B. RBCA oder MFA
- **Verschlüsselung** z.B. während des Datentransfers und /oder der Speicherung
- **Sicherheitsprüfungen** z.B. Pen-Test, Sicherheitsaudits
- **Netzwerksicherheit** z.B. Firewalls, Intrusion Detection Systems (IDS) oder Intrusion Prevention Systems (IPS)
- **Datensicherung** z.B. Backup-Konzepte, Disaster Recovery Pläne
- **Überwachung** z.B. menschliche Aufsicht
- **Schulung und Awareness**
- **Meldepflichten**



Bedrohungen
und Risiken

Regelwerkserstellung und Dokumentationsanforderungen zur Nutzung von KI

*Beispiel



Umsetzungsfristen

KI -VO

In Kraft seit 01. August 2024 mit
einer zweijährigen
Übergangsfrist (2026)

In Teilen bereits ab 2025 gültig

KI-Kompetenz 2. Februar 2025

Regeln zu GPAI 2. August 2025

DORA-VO

In Kraft seit 16. Januar 2023 mit
einer zweijährigen Übergangsfrist

Gilt ab 17. Januar 2025

NIS-2

Deutsches Umsetzungsgesetz seit
dem 06.12.2025 in Kraft

Grundsätze zur Nutzung von KI im Unternehmen

1. Geben Sie KI-Ergebnisse nicht als eigene Arbeitsergebnisse/Leistungen aus!
2. Gehen Sie nicht davon aus, dass KI perfekt ist und fehlerfreie Ergebnisse produziert!
3. Füttern Sie die KI nicht mit sensiblen Daten- die KI gibt nicht, sie nimmt auch!
4. Überlegen Sie, ob Sie Ihre Datenbank/Webseite der KI schenken wollen. Nutzen Sie Opt-Out-Optionen!
5. Verwenden Sie nicht unbedacht Prompts zu Personen und Marken!
6. Lesen Sie die Bedingungen des KI-Einsatzes: Wem gehören Input und Output?
7. Setzen Sie KI-Ergebnisse nie unbedacht über API-Schnittstellen oder anderweitig automatisiert als Host ein!
8. Setzen Sie die KI-Ergebnisse nie unbedacht im Personalbereich ein!
9. KI ist nicht generell verboten und auch nicht generell schlecht: Denken Sie an die Compliance!
10. Halten Sie sich über rechtliche Regelungen auf dem Laufenden!

Steigt der Stromverbrauch durch KI?

- ✓ Der globale Stromverbrauch von KI-Rechenzentren wird von 2023 bis 2030 voraussichtlich um das Elffache auf etwa 550 Milliarden Kilowattstunden ansteigen.
- ✓ Der hohe Energiebedarf führt zu erheblichen CO₂-Emissionen. Zudem wird zur Kühlung der Server eine riesige Menge Wasser verbraucht, was sich bis 2030 in etwa vervierfacht.
- ✓ Eine ChatGPT Anfrage soll so viel **Energie** verbrauchen wie eine Sekunde Backofen-Betrieb.
- ✓ Aber: Optimierungen, wie mathematisch effizientere Verfahren, können den Energieverbrauch laut Studien um bis zu 90 Prozent senken.



STEPHAN AUGE
Teamleiter
Managementsysteme
& Prokurist



migosens GmbH
Wiesenstraße 35
45473 Mülheim an der Ruhr
+49 208 / 99395110
stephan.auge@migosens.de

► Offene Themen und Fragen

