managementsysteme
by migosens

WISSENSAUSTAUSCH „EINSATZ VON KI UND NEUE ANFORDERUNGEN 2025“

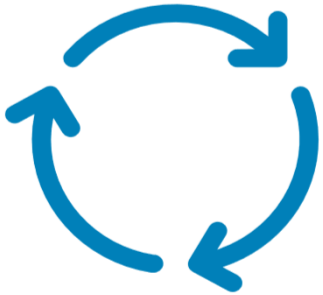
EINE HERAUSFORDERUNG ZUR ERFÜLLUNG DER COMPLIANCE IM HINBLICK AUF DIE REGULATORISCHEN UND GESETZLICHEN ANFORDERUNGEN ZUR CYBERRESILIENZ, DIGITALEN SICHERHEIT UND ZUM DATENSCHUTZ

22.11.2024

www.migosens.de

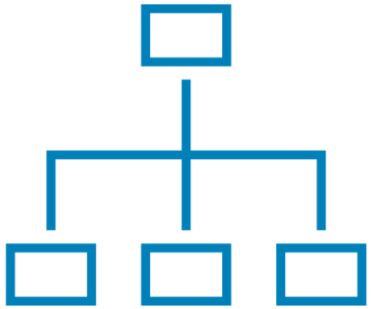
Anforderung an die Implementierung gem. KI-VO

managementsysteme by migosens



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

Schulung und Awareness sowie Informationspflichten

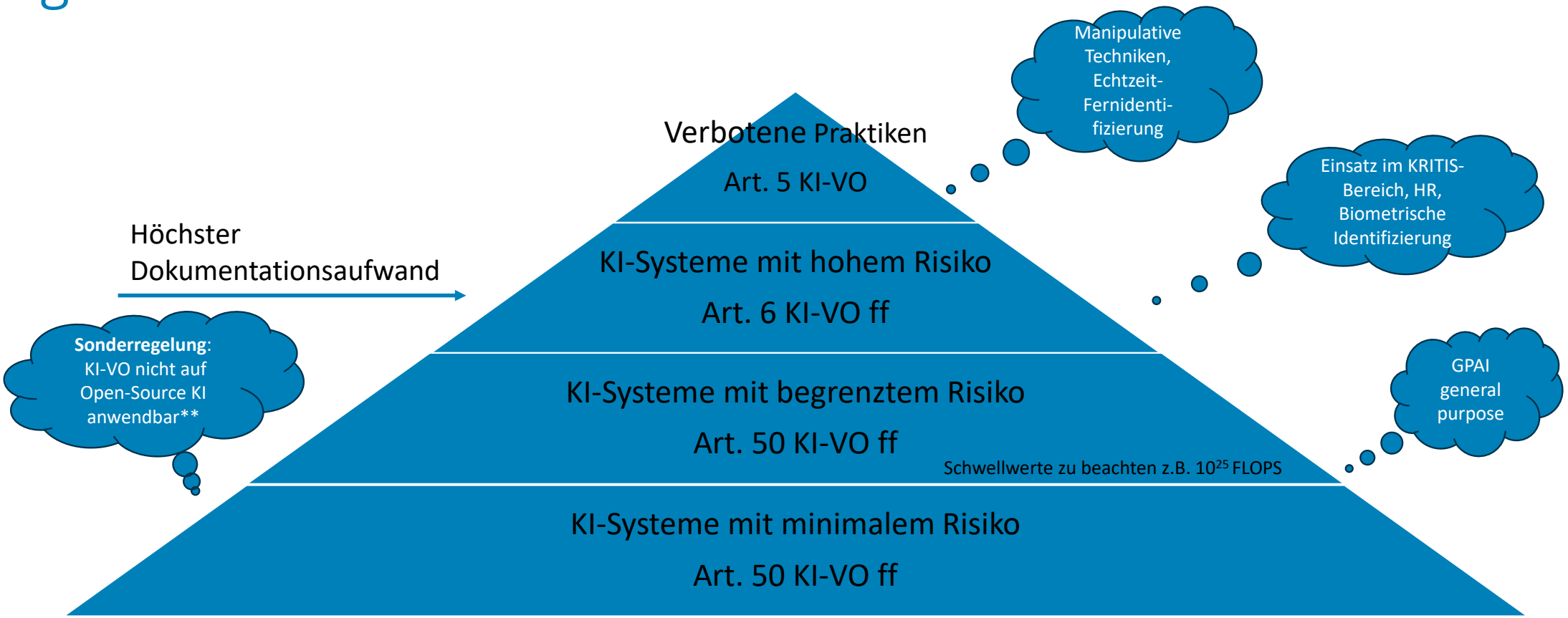
- Art. 4 KI-VO
- Art. 26 Abs. 2 und Abs. 7 KI-VO

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

KI-Systeme _Risikobasierter Ansatz gem. KI-VO

managementsysteme by migosens



**Ausnahme gilt nicht wenn verbotene Praktiken, Hochrisiko-KI-Systeme und jene bestimmte KI-Systeme, die für Art. 50 KI-VO Anbietern und Betreibern Transparenzpflichten auferlegt – siehe Art. 2 Abs. 12 KI-VO

*FLOPS= Floating Point Operations per Second = Einheit zur Leistungsfähigkeit von Computern

Risikobewertung und –management gem. Art. 9 KI-VO

managementsysteme by migosens

Identifikation von Risiken

- Analyse von pot. Sicherheitsrisiken z.B. Datenlecks, Cyberangriffe

Risikominderungsstrategien

- Entwicklung von Strategien zur Risikoreduktion z.B. Sicherheitsmaßnahmen und Überwachung

Bedeutung für die Informationssicherheit/ Cyberresilienz

managementsysteme by migosens

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, Desaster Recovery Pläne
- **Überwachung** z.B. menschliche Aufsicht
- **Schulung und Awareness**
- **Meldepflichten**

Bedrohungen und Risiken

Bedeutung für den Datenschutz

managementsysteme by migosens

Datenminimierung

Rechtmäßigkeit und Zweckbindung

Betroffenenrechte

(Transparenz und Informationspflichten)

Datensicherheit (TOM)

Schnittstelle ISMS

Risikobewertung (DSFA)

Meldepflichten

Schnittstelle ISMS

Bedeutung für Ethik-Richtlinien und Unternehmensverantwortung © Co-Pilot (Inhalt)

managementsysteme by migosens

Ethik *(vieles existiert bereits im GG ! – Art. 27 Abs. 2 KI-VO, Bias Art. 10 Abs. 2 lit. f+g und Art. 15 KI-VO Datentransparenz und Robustheit)

- Vermeidung von Diskriminierung und Bias, Sicherstellung von Fairness und Transparenz

Unternehmensverantwortung *(Art. 4 KI-VO gilt grundsätzlich bei allen KI-Systemen- steht vor der Klammer!!)

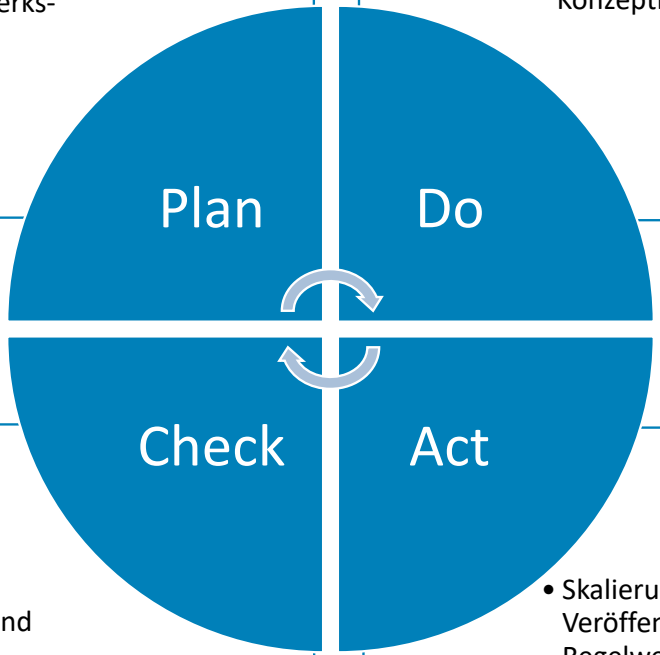
- Berücksichtigung der gesellschaftlichen Verantwortung, Sicherstellung und Förderung der regelkonformen Nutzung von KI

Schritte zur erfolgreichen Implementierung

managementsysteme by migosens

- Juristische Vorklärung
- Definition Zweck(e) KI-Einsatz
- BR/PR informieren*

- Bedarfsanalyse und Entwurf Regelwerks-Erstellung
- Schnittstellen



- Pilotierung und Konzeptionierung

- IT-Sicherheit (TOM)
- Prüfung KI-Anbieter
- Risikomanagement
- Vertragsgestaltung

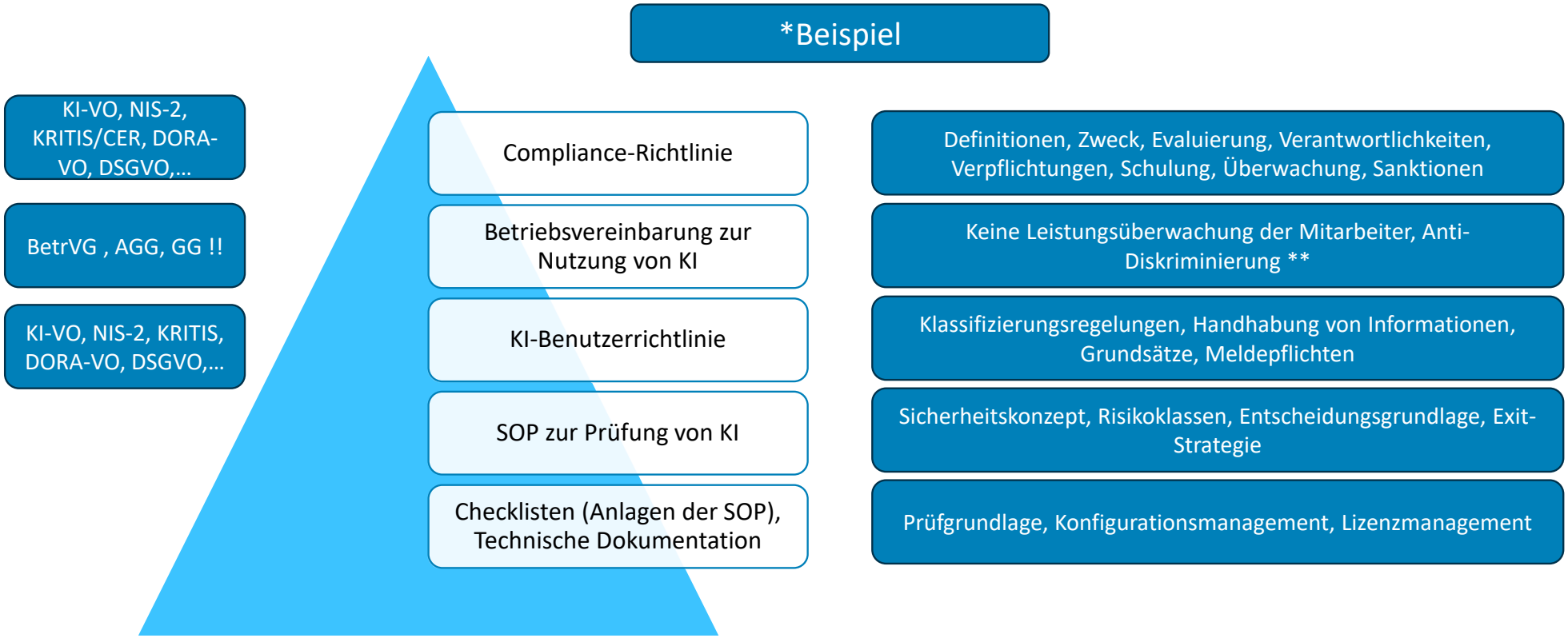
- Laufende Compliance
- Ständiges Update
- Qualitätssicherung

- Kontinuierliche Überwachung und Anpassung

- Skalierung und Veröffentlichung des Regelwerks
- KI-Kompetenz

- Einführungsphase
- Regelwerks-einführung
- Schulung/ Awareness

Regelwerkserstellung und Dokumentationsanforderungen zur Nutzung von KI



Herausforderung Löschkonzept KI– Recht auf Vergessenwerden

managementsysteme by migosens

Kategorie 1 der Entwicklung

Ansatz, bei dem das Recht auf Vergessenwerden bereits beim Training der Systeme berücksichtigt wird

Methoden:

- **Tokenisierung,** Substitution sensibler Daten durch nicht-sensible Äquivalente (Wert ohne Bedeutung)
- **Anonymisierung**
- **Differential Privacy,** Hinzufügen eines Grundrauschen zu den Datensätzen, sodass ein einzelner Datenansatz statistisch nicht erkannt wird

Kategorie 2 der Entwicklung

Ansatz, bei dem bestimmte Teile des KI-Wissens gezielt entfernt werden können, nachdem diese trainiert wurden

Methoden:

- **Maschinelles Vergessen,** Möglichkeit der Entfernung eines einzelnen oder mehrerer Datenpunkte der Trainingsdaten des KI-Systems, ohne dessen Funktionsweise zu beeinträchtigen

z.B. der SISA-Ansatz (Sharded, Isolated, Sliced and Aggregated), der Algorithmus teilt den Trainingsdatensatz in überlappende Teilmengen und trainiert so separate Modelle auf diese Teilmengen, Löschungen können somit auf den betroffenen Teilmengen vorgenommen werden

Quelle: Barenkamp, M., 2024

Herausforderung Compliance - Ausschnitt

managementsysteme by migosens

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**

Herausforderung Compliance - Meldepflichten

managementsysteme by migosens

Schlüsselprozess Meldewesen:

Übersicht der Meldepflichten und Fristen

DSGVO

Behörde:

Landesaufsichts-Behörde

Was:

Datenpannen gem. Art. 33 ff DSGVO

unverzüglich, jedoch max. binnen 72h

NIS-2

Behörde:

BSI

Was:

Stör- und Sicherheitsvorfälle Netz/Informationssysteme

KRITIS-DACH/CER

Behörde:

BBK

Was:

Stör- und Sicherheitsvorfälle KRITIS-Anlagen gem. Art 15, 17 RCE

Gemeinsam eingerichtete Meldestelle (BSI/BBK)

1. Stufe Erstmeldung : unverzüglich, spätestens 24h nach Kenntniserlangung
2. Stufe Meldung: unverzüglich, spätestens 72h nach Kenntniserlangung
3. Stufe Abschlussmeldung: 1 Monat nach Übermittlung der Meldung

3-stufiges Melderegime

DORA-VO

Behörde:

BaFin

Was:

(Schwerwiegende) IKT-bezogene Vorfälle Art. 3 Nr. 8 bzw. Nr. 10 (RTS)

3-stufige Meldung (auch an Kunden)

1. Stufe Erstmeldung : unverzüglich, spätestens 24h nach Feststellung (4h)
2. Stufe Zwischenmeldung, spät. 72h nach Erstmeldung
3. Stufe Abschlussmeldung: 1 Monat nach letzter Zwischenmeldung

Sonderfall wenn NIS-2/DORA gilt:**

KI-VO

Behörde:

Marktaufsichtsbehörde

Was:

Schwerwiegende Vorfälle bei Hochrisiko-KI-Systemen gem. Art. 73 KI-VO

unverzüglich, jedoch max. binnen 15 Tage (10 Tage bei Tod)

Lex-speciales-Regelung, BaFin meldet an weitere Stellen z.B. EZB, ENISA

**NIS2UmsuCG §35 Abs. 2 ENTWURF

Umsetzungsfristen *Stand Nov 2024

managementsysteme by migosens

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 und CER
Gesetzeslage weiter beobachten

Unique selling point- migosens Managementsysteme

Der Lösungsansatz

managementsysteme by migosens

Ganzheitliche Compliance Sicherstellung

Grundlage :

- **Systematischer Ansatz,** Managementsystem, Regelwerksverfolgung (Rechtskataster)
- **Effektives Risikomanagement,** DRM und ZRM
- **Strukturiertes Dokumentenmanagement,** Wissenstransfer
- **Angemessenes Schulungskonzept,** Wissenserwerb, Kompetenz-Aufbau
- **Effektive Kommunikationsstrategie,** Verantwortlichkeiten und Meldewesen
- **Kontinuierliche Überwachung,** Anpassung und Verbesserung

Unique selling point- migosens Managementsysteme

Der Lösungsansatz

ISO 9001, ISO 27001

QMS (9001) bzw. ISMS-Basis (27001) bzw. das Fundament, dass genutzt werden kann, um KI sicher und effizient im Unternehmen einzuführen und zu verwalten

Grundlage:

- **Risikomanagement**
- **PDCA**
- **Meldewesen**

ISO 42001

Ausbau des Produktportfolios um das Managementsystem ISO/IEC 42001:2023-12 Informationstechnik- Künstliche Intelligenz-Managementsystem (KIMS)

Anforderung:

- **Regulatorische, gesetzliche Anforderungen**
- **Normative Anforderungen**
- **Gesellschaftliche Anforderungen, Marktanforderung**

Zu guter Letzt- Schlaglichter

managementsysteme by migosens

KI und das UrhG
nach § 2UrhG ist nur eine menschliche Schöpfung urheberrechtlich geschützt, aber Achtung: Service-Anbieter kann Rahmenbestimmungen vorgeben

KI und Weitergabe von Daten
Prüfen, inwiefern der Lizenzgeber die Rechte an den Ergebnissen an den Lizenznehmer überträgt (z.B. bei Microsoft)

Rechte Dritte
Insbesondere bei Bildern ist die Verletzung Rechte Dritter nicht auszuschließen, wenn deren Daten zu Trainingszwecken verwendet wurden

KI und BR
Vorgaben des Arbeitgebers zur Nutzung von ChatGPT und vergleichbaren Tools lösen je nach Sachverhaltsebene kein zwingendes Mitbestimmungsrecht des BR aus

KI und das BetrVG
§ 87 Abs. 1 Nr. 6 BetrVG ist bei der Nutzung von ChatGPT nur dann einschlägig, wenn der durch Datenspeicherung ggf. erzeugte Überwachungsdruck vom Arbeitgeber ausgeht und überwachbare Accounts vorliegen

KI und die DSGVO
Bei der Festlegung der Rechtsgrundlage ist die Geeignetheit und Erforderlichkeit der Verarbeitung vordergründig, KI selbst ist nur ein besonderes Mittel und irrelevant aufgrund Technologieneutralität

Back-up

Grundsätze zur Nutzung von KI im Unternehmen

Erfolgreiche Anwendungsbeispiel von KI im IT/OT-Bereich

Unterstützung von KI im ISMS-Kontext

Grundsätze zur Nutzung von KI im Unternehmen

managementsysteme by migosens

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!

Quelle: Wilmer, T. 2024

Erfolgreiche Anwendungsbeispiele von KI im IT- und OT-Bereich © Co-Pilot (Inhalt)

managementsysteme by migosens

IT-Bereich

- **Predictive Maintenance:** Einsatz von KI zur Vorhersage und Vermeidung von Systemausfällen
- **Cybersecurity:** Nutzung von KI zur Erkennung und Abwehr von Cyberangriffen, Anomaliererkennung 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

Unterstützung von KI im ISMS-Kontext © Co-Pilot (Inhalt)

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

Quellenangaben

Mit © Co-Pilot markierte Textpassagen entstammen vom Inhalt der KI Co-Pilot

Haufe Akademie, Whitepaper- „Den AI Act verstehen- Rechte und Pflichten kennen“

Gehring, P., Können lernende Systeme neutral sein- Zum Problem der Verzerrungen (Biases) und dem Ruf nach Ethik“, DuD, 08/24

Bortinikov, V., Dukart, J., Informationelle Selbstbestimmung und KI, Datenschutzrechtliche Anforderungen an die Transparenz von KI, ZD, 10/24

Wilmer, T., Künstliche Intelligenz & Recht, 2024

Reichert, F. et al. KI-Verordnung: Rechtsgrundlagen für die Bereitstellung und Nutzung von KI, ZD 09/24

Barenkamp, M., KI-Systeme und das Recht auf Vergessenwerden, PinG, 05/24

ArbG Hamburg „Einsatz von Künstlicher Intelligenz im Unternehmen“ Beschluss v. 16.1.24- 24 BVGa 1/24