Bundesnetzagentur

NETZWERKTREFFEN

Netzwerktreffen | Bedeutung der KI-Normung für Unternehmen

09. Dezember 2025
9:00 – 10:30 Uhr

Agenda:

1. **Begrüßung und Einführung**

2. **Überblick: Aufgaben der BNetzA im Bereich der KI-Standardisierung**
   Dieter Penning, BNetzA
3. **Normen im Bereich Risikomanagement, Qualitätsmanagement und Cybersicherheit**
   Annegrit Seyerlein-Klug, Technische Hochschule Brandenburg
4. **Beteiligungsprozess an der Normung**

Bundesnetzagentur

Aufgaben der Bundesnetzagentur zur KI-Standardisierung

Dieter Penning, Bundesnetzagentur

Netzwerktreffen der Abt 9

Online-Meeting, 09. Dezember 2025

Aufgaben der Bundesnetzagentur zur KI-Standardisierung

KI-Standardisierung (1)

- Der Fokus der KI-Standardisierung liegt auf zehn Themenfeldern, die in dem Standardisierungsmandat der Europäischen Kommission definiert sind.
  - Ziel des Mandats ist es, harmonisierte Normen zu schaffen, welche eine zentrale Rolle bei der Umsetzung der Verordnung (EU) 2024/1689 (KI-VO) spielen.
- Artikel 40 der KI-VO legt den Rahmen für harmonisierte Normen und weitere Normungsdokumente im Kontext der KI-VO fest.
  - Er definiert, wie Konformität mit harmonisierten Normen zur Erfüllung der Anforderungen aus der KI-VO hergestellt werden.
- Die Einhaltung dieser Normen schafft eine Konformitätsvermutung.
  - KI-Systeme, die den harmonisierten Normen entsprechen, gelten als konform mit den entsprechenden technischen Anforderungen der KI-VO und schafft insbesondere Rechtssicherheit für die Hersteller.

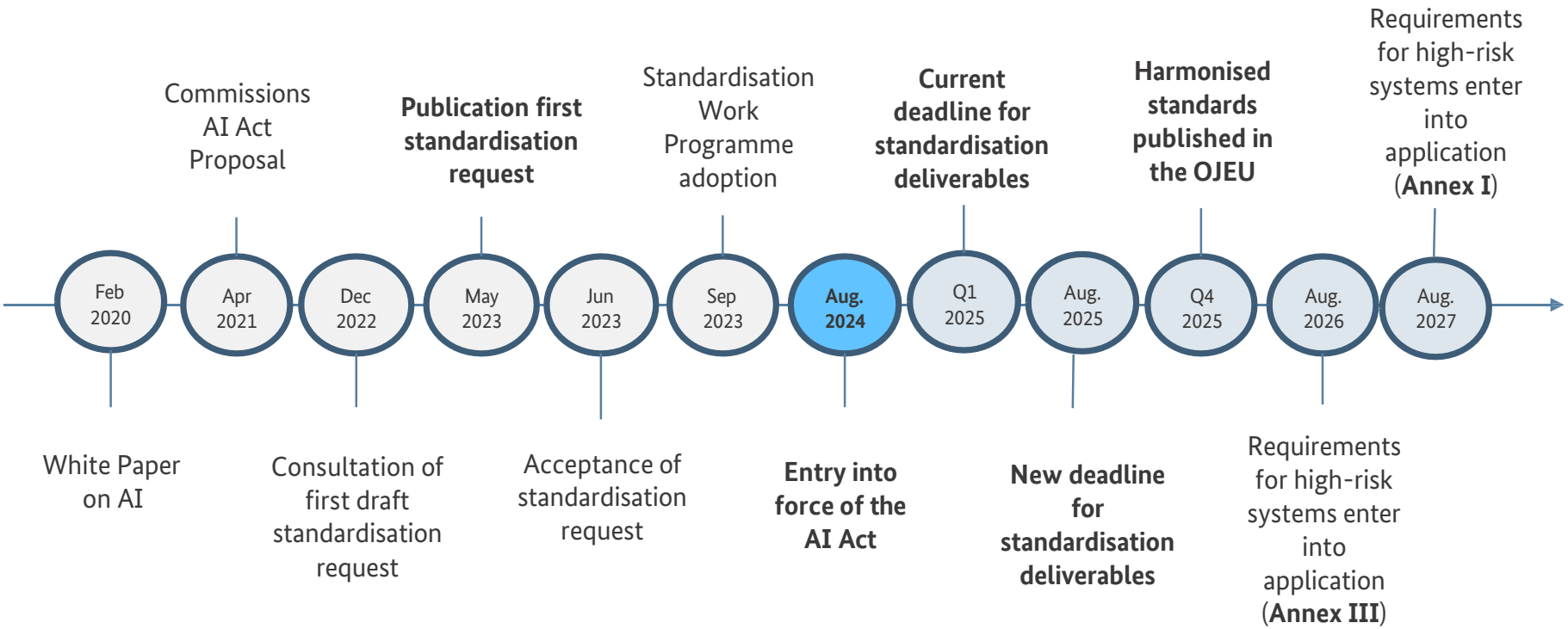
KI-Standardisierung (2)

- Bei der KI-Standardisierung sind technologische, gesellschaftliche, rechtliche und ethische Aspekte zu berücksichtigen, wie sie in der KI-VO festgelegt sind.
- Die Normen bieten praktische Anleitungen und technische Vorgaben, die Unternehmen bei der Entwicklung und dem Einsatz von KI-Systemen unterstützen. Sie helfen dabei, die in der KI-VO festgelegten Anforderungen in die Praxis umzusetzen.
- Diese Anforderungen beziehen sich auf Risikomanagement, Datenqualität und Daten-Governance, technische Dokumentation, Aufzeichnungspflichten und Transparenz.
- Förderung von Innovationen im KI-Bereich und schaffen fairen Wettbewerb im europäischen Binnenmarkt zu gewährleisten.
- Die Bundesnetzagentur wird hierzu auf die deutschen Akteure in der Standardisierung zugehen, um Interessen abzugleichen und Anregungen für ein gemeinsames Verständnis zu geben.

Der Fokus der KI-Standardisierung liegt auf zehn Themenfeldern aus dem Standardisierungsmandat

- Risikomanagement für KI-Systeme
- Aufzeichnung durch Protokollierungs-funktionen von KI-Systemen
- Spezifikationen für die Robustheit von KI-Systemen
- Regulierung und Qualität von Datensätzen, die zur Entwicklung von KI-Systemen verwendet werden
- Menschliche Aufsicht über KI-Systeme
- Konformitäts-bewertung für KI-Systeme
- Transparenz und Information für Nutzer von KI-Systemen
- Spezifikationen für die Cybersicherheit von KI-Systemen
- Spezifikationen für die Genauigkeit von KI-Systemen
- Qualitätsmanagement-systemen für Anbieter von KI-Systemen, einschließlich Verfahren zur Beobachtung nach dem Inverkehrbringen

Angedachter Zeitplan: KI-Standardisierung



Quelle: AI Office

-> Other standardisation requests may be published in the future

Die KI-Verordnung ist stufenweise anwendbar

Digital Omnibus on AI Regulation: Backstop-Termine sind **unverrückbare** Deadlines, selbst wenn Standards noch nicht finalisiert sind.

01.08.2024

In Kraft getreten

02.02.2025

- KI-Kompetenz
- verbotene Praktiken im KI-Bereich

02.08.2025

- KI-Modelle mit allg. Verwendungszweck
- Benennung der nationalen Behörden - Marktüberwachung sowie Notifizierung
- Zentrale Anlaufstelle
- Sanktionen

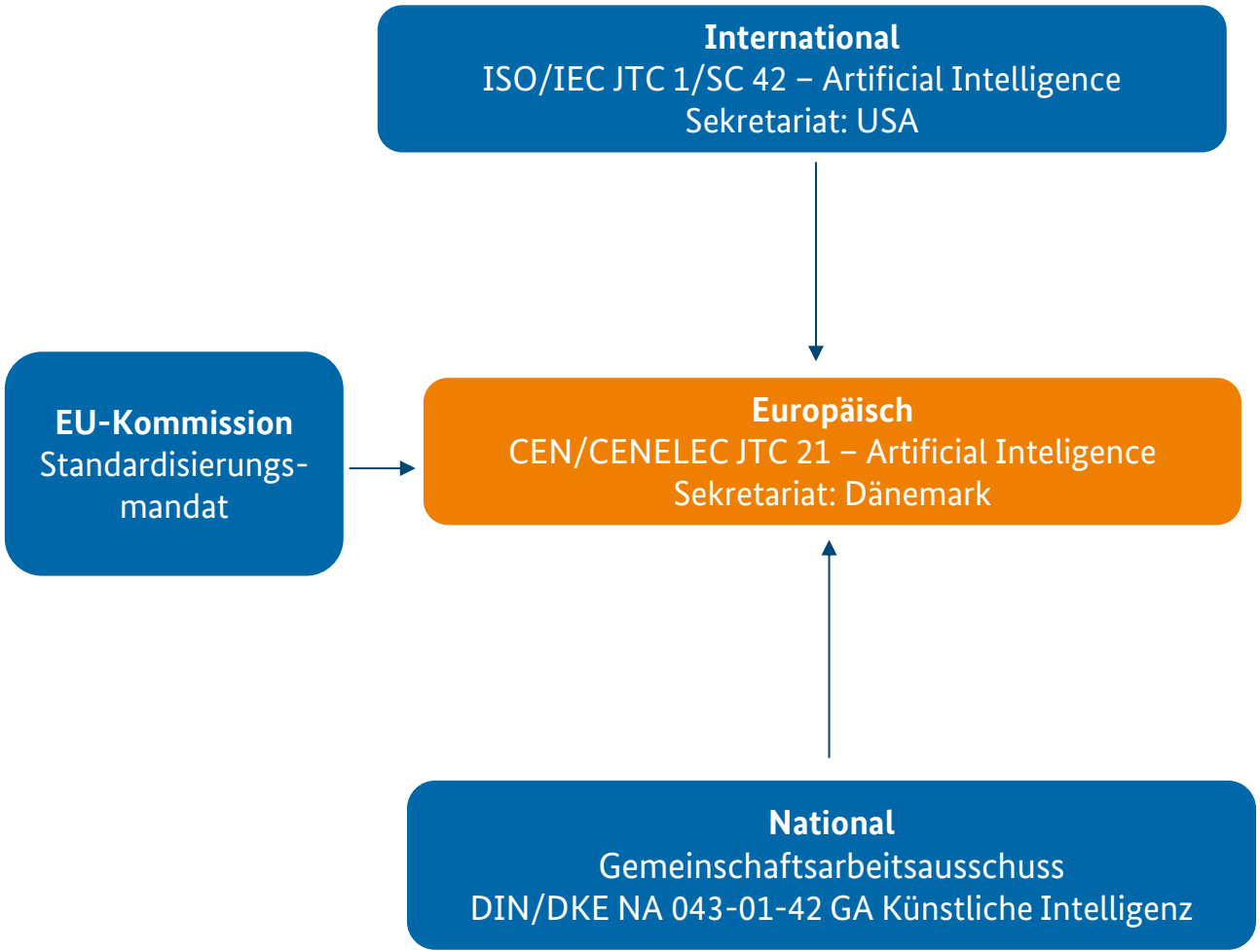
02.08.2026 → **02.12.2027 (letzter Zeitpunkt)**

Allgemeine Anwendbarkeit, u.a.:

- Hochrisiko-KI-Systeme, Anhang III
- Transparenz-Gebote
- Reallabor

02.08.2027 → **02.08.2028**

- Hochrisiko-KI-Systeme, die in Produkten integriert sind; Auflistung im Anhang I



Stand Dezember 2025:
- 51 Mitgliedsländer und 26 Beobachterstaaten
- 41 internationale Standards zu KI wurden mittlerweile entwickelt
- aktuell 47 Standards in Entwicklung
- Gemeinsame Projekte mit CEN/CENELEC

- entwickelt KI-Standards zur Untermauerung des AI-Act nach 10 Themen (Normungsmandat)
- Internationale Standards werden übernommen oder modifiziert
- 9 europäische Standards derzeit in der Entwicklung

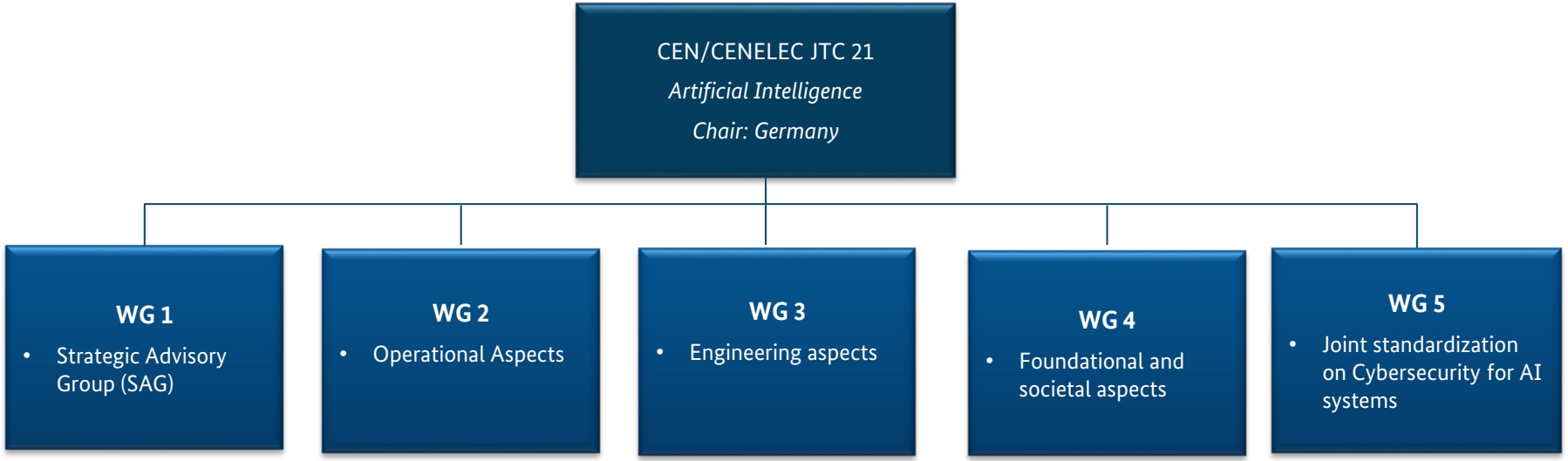
AK 2: Grundnormen
und Konformität
AK 3: Daten
AK 4: Vertrauenswürdigkeit
AK 5: Cybersicherheit

Aktualisierter·Zeitplan·in·der·JTC·21

JTC 21 homegrown standards in support of the AI Act

Note: CEN/CENELEC publication is different than the citation in the OJEU which may take additional weeks or months.

KI-Gremien - europäisch



Anmerkungen

- Working Groups im JTC 21 bilden i.d.R. „Task Groups“ zur Bearbeitung einzelner Projekte
- Die WG 1 leistet selbst keine Standardisierungsarbeit

First batch of enquiries to be circulated mid February 2026

WG 2 "Operational aspects„
JT021024: prEN 18228 "AI Risk Management"
Comment Resolution Meetings on WD from 16 November 2025 to 12 February 2026
Enquiry process to start 13 February 2026

JT021038: prEN 18285 "AI Conformity assessment framework"
Comment Resolution Meetings on WD from 15 January to 14 February
Enquiry process to start 17 February 2026

WG 3 "Engineering aspects"
JT021025: prEN 18281 "Artificial Intelligence – Evaluation methods for accurate computer vision systems"
Comment Resolution Meetings on WD from 18 December 2025 to 9 February 2026
Enquiry process to start 12 February 2026

First batch of enquiries to be circulated mid February 2026

WG 4 “Foundational and societal aspects”

JT021008: prEN 18229-1 "AI trustworthiness framework – Part 1: Logging, transparency and human oversight"

Comment Resolution Meetings on WD from 16 November 2025 to 12 February 2026
Enquiry process to start 15 February 2026

JT021047: prEN 18229-2 "AI trustworthiness framework – Part 2: Accuracy and robustness"

Comment Resolution Meetings on WD from 13 January 2026 to 12 February 2026
Enquiry process to start 15 February 2026

WG 5 "Joint standardization on Cybersecurity for AI systems"

JT021029: prEN 18282 "Artificial intelligence – Cybersecurity specifications for AI Systems"

Comment Resolution Meetings on WD from 16 November 2025 to 12 February 2026
Enquiry process to start 15 February 2026

Second batch of enquiries to be circulated mid June 2026

WG 3 "Engineering aspects"

JT021036: prEN 18283 "Artificial Intelligence – Concepts, measures and requirements for managing bias in AI systems"

Comment Resolution Meetings on WD from 3 March 2026 to 12 June 2026

Enquiry process to start 15 June 2026

JT021037: prEN 18284 "Artificial Intelligence – Quality and governance of datasets in AI"

Comment Resolution Meetings on WD from 3 March 2026 to 12 June 2026

Enquiry process to start 15 June 2026

KI-Gremien - national

- Folgende Gremien werden in Deutschland gespiegelt:
  - NA 043-01-42 GA „Künstliche Intelligenz“,
    - AK 1: KI-Qualität und Prüfverfahren
    - AK 2: Grundlegende Standards und Konformität
    - AK 3: Daten
    - AK 4: Vertrauenswürdigkeit
    - AK 5: Cybersicherheit

Anmerkungen:

- AK 1 ist nicht aktiv, Themen werden in den AKs 2 und 4 behandelt

- Das Engagement im Bereich der KI-Standardisierung ist weiter zu intensivieren!

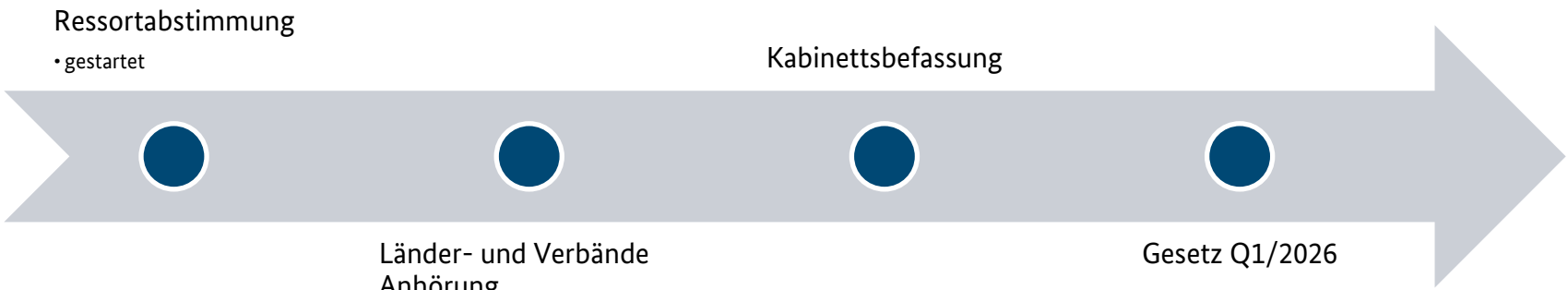
Wer macht bei den Standards mit?

- Industrie und Handel, inkl. KMU
- Forschungsinstitute, Universitäten, Hochschulen
- Öffentliche Hand, Bundesbehörden
- Gewerkschaften
- Stiftungen
- Organisationen für Zertifizierung, Audits
- Verbände

Gestalten Sie die KI-Zukunft mit!

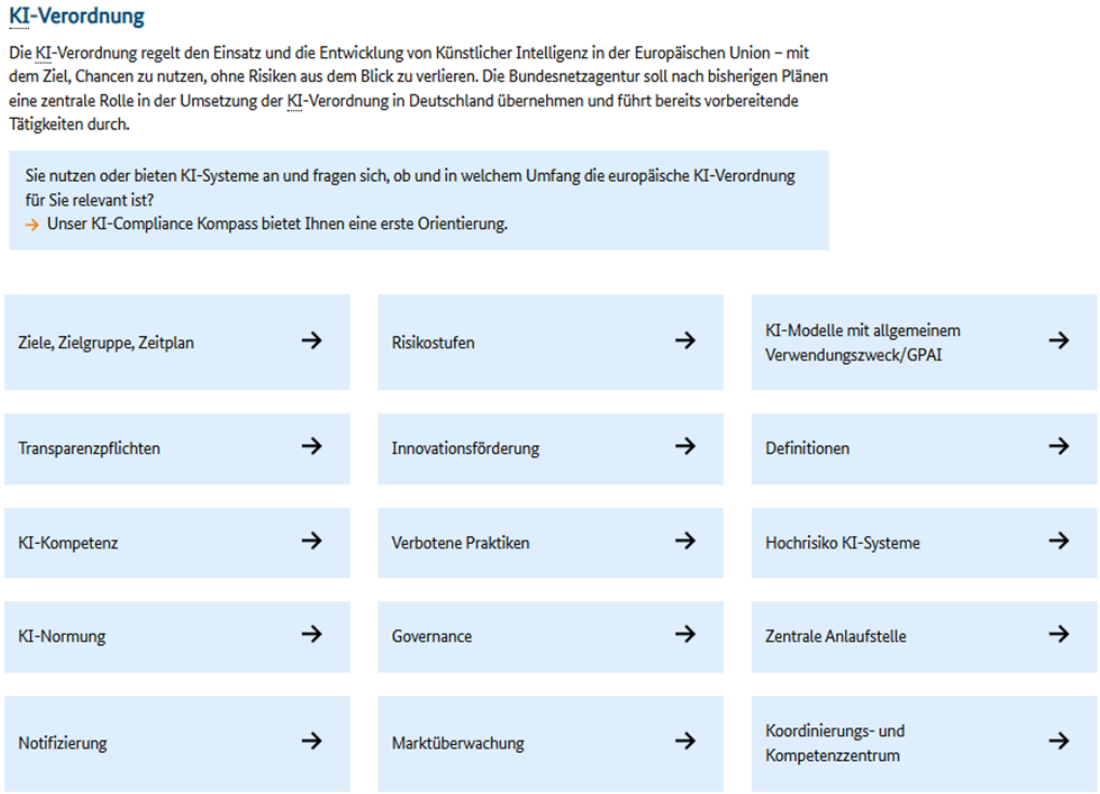
Stand der vorbereitenden Arbeiten bei der Bundesnetzagentur

Nationales Durchführungsgesetz zur KI-Verordnung



KI-Service Desk

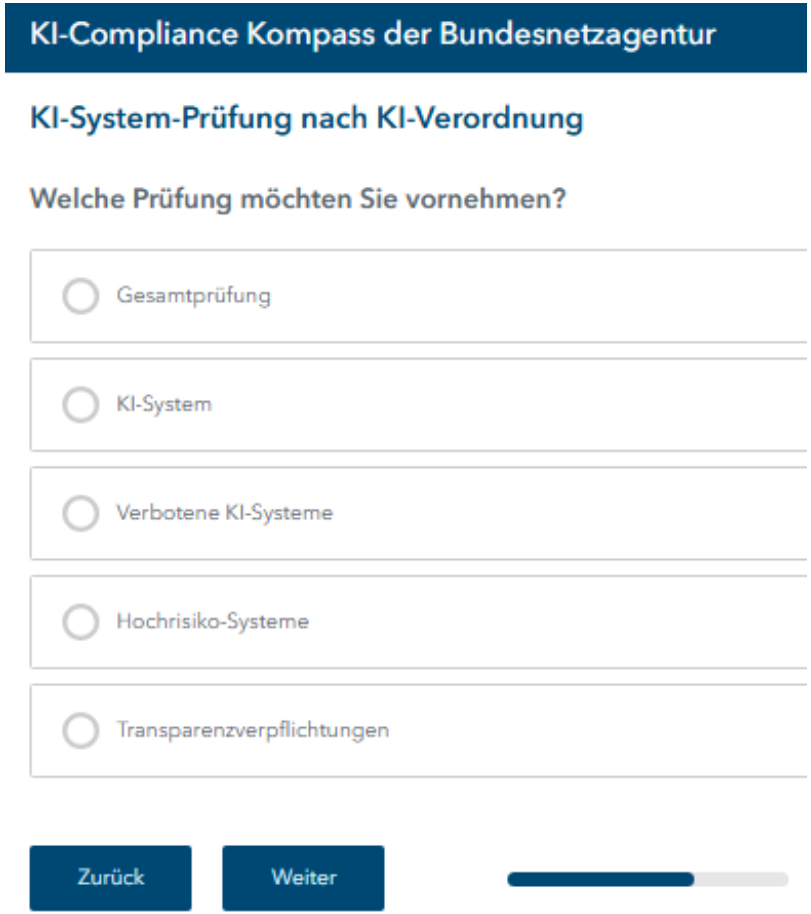
KI-Service Desk



- ✓ Für mehr Rechtsicherheit der Marktteilnehmer
- ✓ Breit angelegtes Informationsangebot
- ✓ Unsicherheiten entgegenwirken
- ✓ Proaktive Kommunikation

www.BNetzA.de/KI

KI-Compliance Kompass



- ✓ Gesamtcheck für alle nachfolgend genannten Bereiche
- ✓ Ist mein System ein KI-System im Sinne der KI-Verordnung?
- ✓ Ist das System laut der KI-VO verboten?
- ✓ Ist das System ein Hochrisiko-System?
- ✓ Welche Transparenzverpflichtungen sind zu beachten?

Weitere To-Dos (Auswahl)

Bundesnetzagentur

Vielen Dank für die Aufmerksamkeit!

Dieter Penning
dieter.penning@bnetza.de
www.bundesnetzagentur.de
Tel. +49 6131 18-7055
Mobil +49 173 6795244

GanzheitlicherSicherheitsansatz für Hochrisiko KI-Systeme

Unterstützung durch die Normung

Annegrit Seyerlein-Klug , CEN CENELEC JTC 21Convenor WG 5

1. **Einordnung und Anforderungen**
2. **Beispiel Risikomanagement (RMS)**
3. **Beispiel Qualitätsmanagement (QMS)**
4. **Beispiel Cybersecurity**

Ziel der KI Verordnung für Hochrisiko AI

Art. 1
(1) Zweck dieser Verordnung ist es,

- das Funktionieren des Binnenmarkts zu verbessern und
- die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz (KI) zu fördern und gleichzeitig
- ein **hohes Schutzniveau** in Bezug auf **Gesundheit, Sicherheit (Safety)** und die in der **EU Charta verankerten Grundrechte**, einschließlich **Demokratie, Rechtsstaatlichkeit und Umweltschutz**, **vor schädlichen Auswirkungen von KI-Systemen** in der Union zu gewährleisten und
- die Innovation zu unterstützen.

(2) In dieser Verordnung wird Folgendes festgelegt:

a) harmonisierte Vorschriften (Standards/Normen) für das
- **Inverkehrbringen,**
- **die Inbetriebnahme und**
- **die Verwendung von KI-Systemen** in der Union;

Gesundheit

Physische Sicherheit

EU Charta der Grundrechte

Hintergrund und Zweck im rechtlichen Rahmen (Auszug)

Die **EU-KI-Verordnung (EU) 2024/1689)** verpflichtet Anbieter von **Hochrisiko-KI-Systemen zu:**

Art. 4: Organisation angemessener KI Kompetenzen

Art. 16 definiert **die Pflichten der Anbieter** von Hochrisiko-KI-Systemen für Konformität:

- Erfüllung der organisatorischen und technischen Anforderungen aus Abschnitt 2 **(Artikel 9-15)**
- Qualitätsmanagementsystem entsprechend **Art.17**
- Aufbewahrung von Dokumentationen gemäß **Art.18; 19**

Art. 43 Konformitäts-Assessment;
Art. 47 Konformitäts-Erklärung
Art. 48 CE Kennzeichen
Art. 49 Registrierung

- U.a.m.

Ziel der harmonisierten Standards

Harmonisierte Standards definieren für das Gesetz, hier KI Verordnung

strukturierte, prüfbare Anforderungen im Einklang mit den **Artikeln 9-15 und 17 und sollen**

- ✓ eine verhältnismäßige Anwendung für Organisationen unterschiedlicher Größe und Komplexität gewährleisten.
- ✓ der Konformitätsbewertungen dienen und das Post-Market-Monitoring unterstützen.

Vermutung der Konformität vs. alternative Nachweisführung

➢ **Vermutung der Compliance zum Gesetz durch Konformität:**

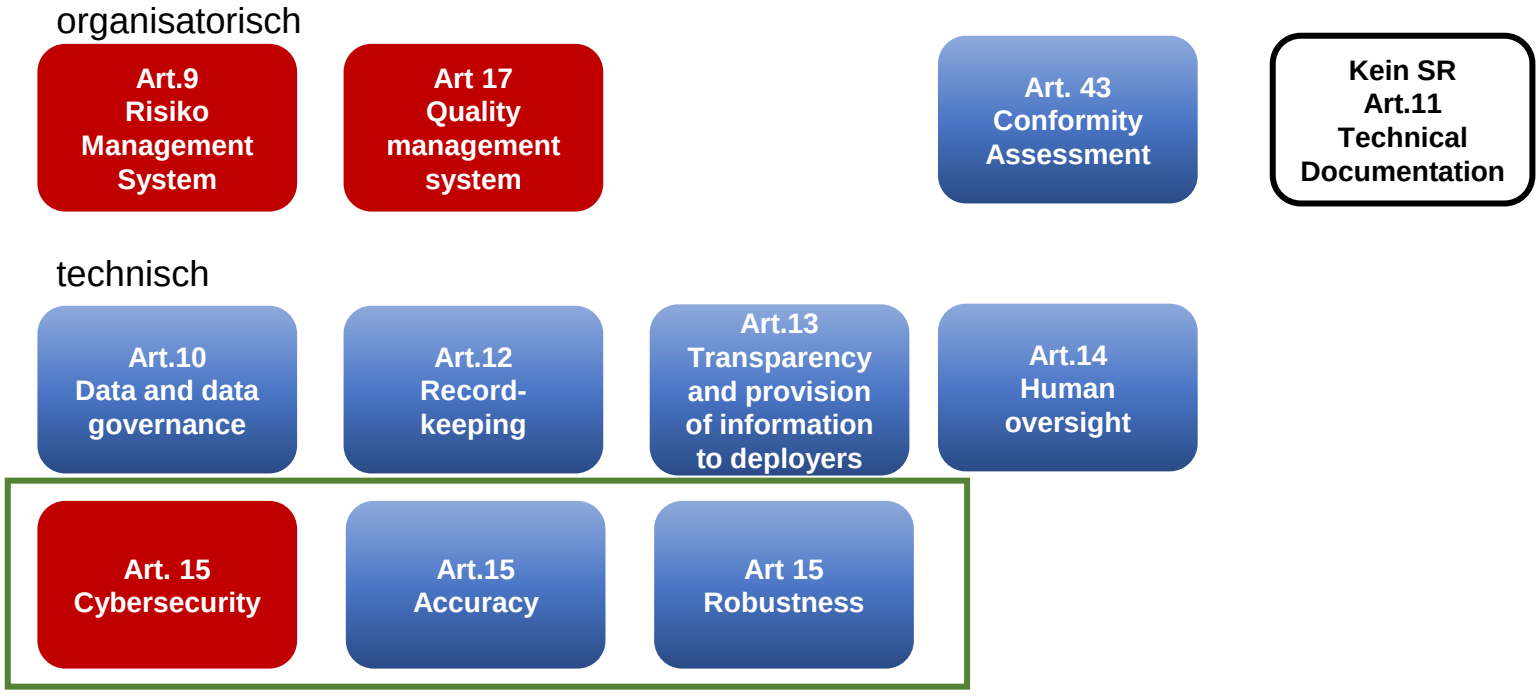
Die Nutzung **harmonisierter Standards (Normen)** gilt automatisch als Nachweis der Einhaltung der entsprechenden Anforderungen der KI-Verordnung, sobald diese im **Amtsblatt der EU (OJEU)** veröffentlicht sind.

➢ **Alternative Nachweisführung:**

Anbieter können andere Verfahren wählen, müssen jedoch jeden rechtlichen Anspruch einzeln nachweisen und dokumentieren.

Die **Europäische Kommission** hat einen **Normungsauftrag** an **CEN/CENELEC** erteilt, um diese **harmonisierten Standards durch die Industrie** für die EU-KI-Verordnung zu entwickeln.

10 Standardisierungsrequests zu Art 9-15 + 17 des AI-Act



Ziel für das KI System

Das KI-System muss im Design, Entwicklung und Betrieb

- robust,
- präzise,
- widerstandsfähig und
- sicher sein.

Es darf keinen schwerwiegenden Schaden (harm) anrichten.

Was ist ein KI System
AI Act Artikel 3 Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „KI-System“

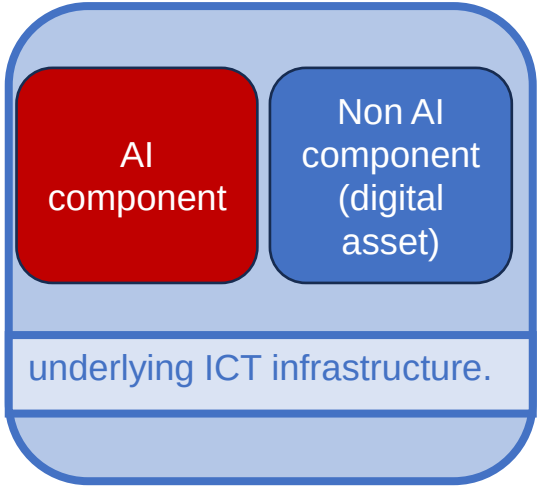
Ist ein **maschinengestütztes** System,

das für einen in unterschiedlichem Grade **autonomen Betriebs ausgelegt ist** und

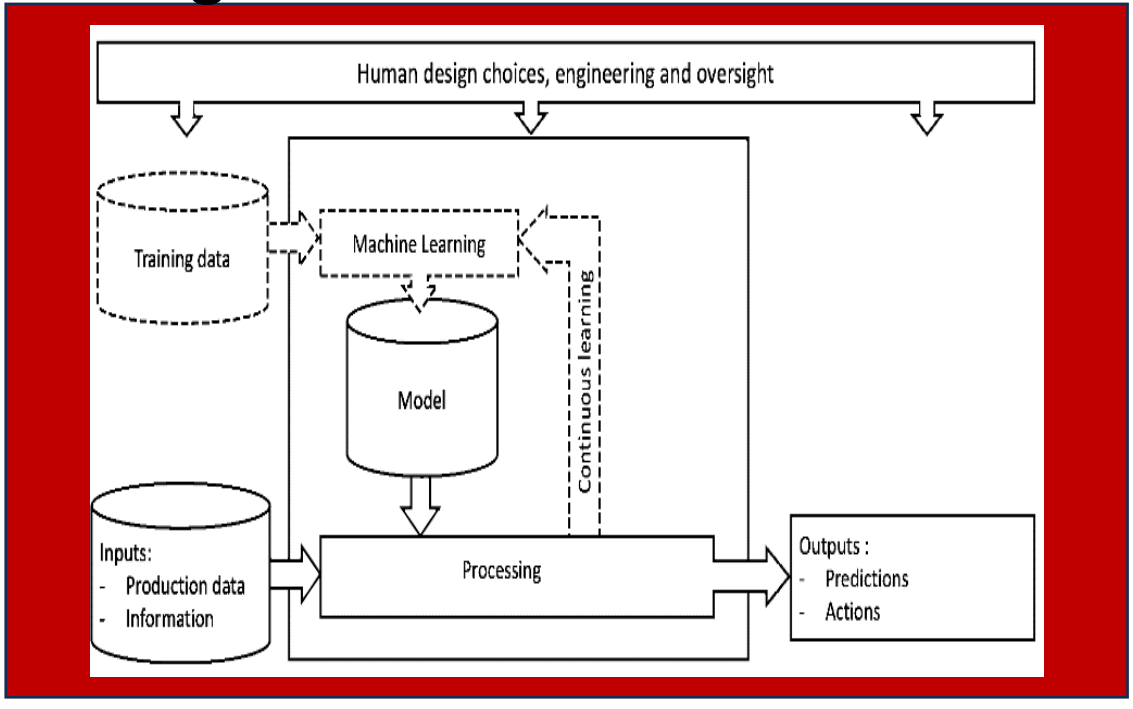
das nach seiner Betriebsaufnahme **anpassungsfähig sein kann** und

das aus den **erhaltenen Eingaben für explizite oder implizite Ziele ableitet**, **wie Ausgaben** wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen **erstellt werden**,

die physische oder virtuelle Umgebungen beeinflussen können;



KI – System gemäß ISO/IEC 22989



Im Kontext KI –VO: KI -Komponente

Cybersecurity Specification for AI systems

1. Einordnung und Anforderungen
2. Beispiel Risikomanagement
3. Beispiel Qualitätsmanagement
4. Beispiel Cybersecurity

Risikomanagement (RMS) Art.9

Kontinuierlicher iterativer Prozess,

der **während des gesamten Lebenszyklus** eines Hochrisiko-KI-Systems geplant und durchgeführt wird und eine regelmäßige systematische Überprüfung und Aktualisierung erfordert.

Risikomanagement

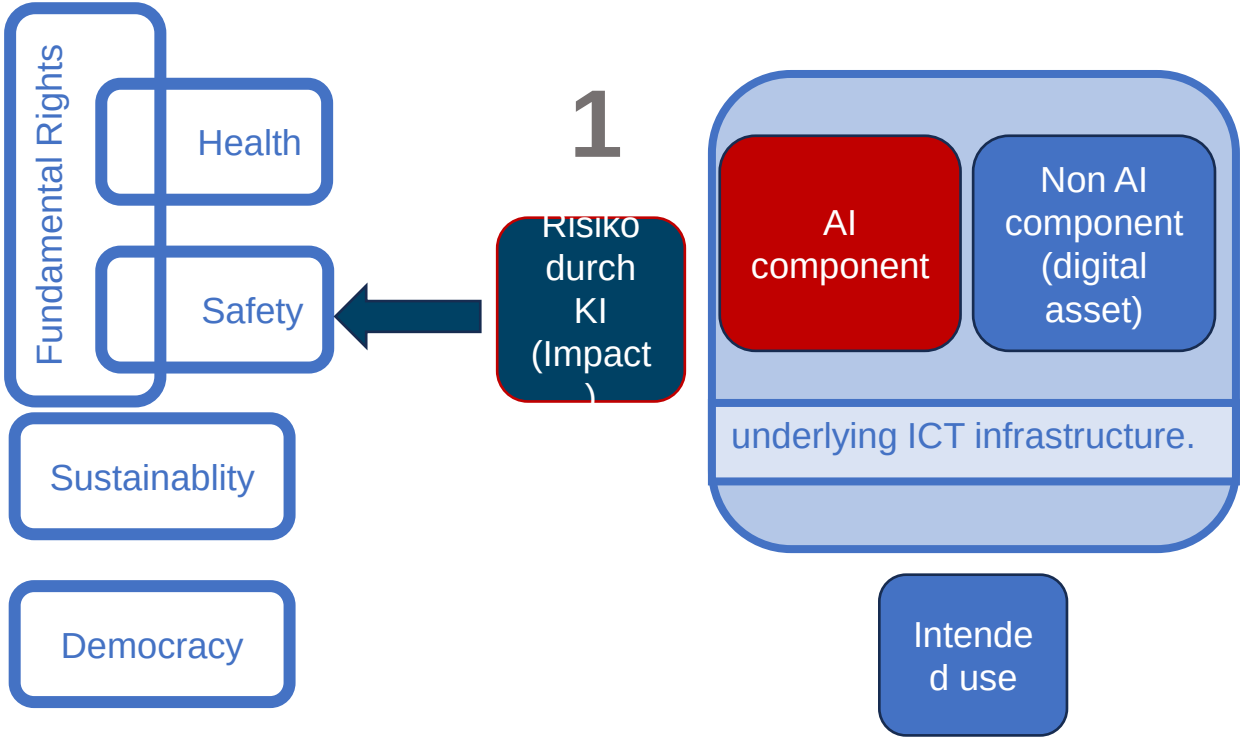
- Ermittlung und Analyse der Risiken
- Abschätzung und Bewertung der Risiken
- Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen

Tests

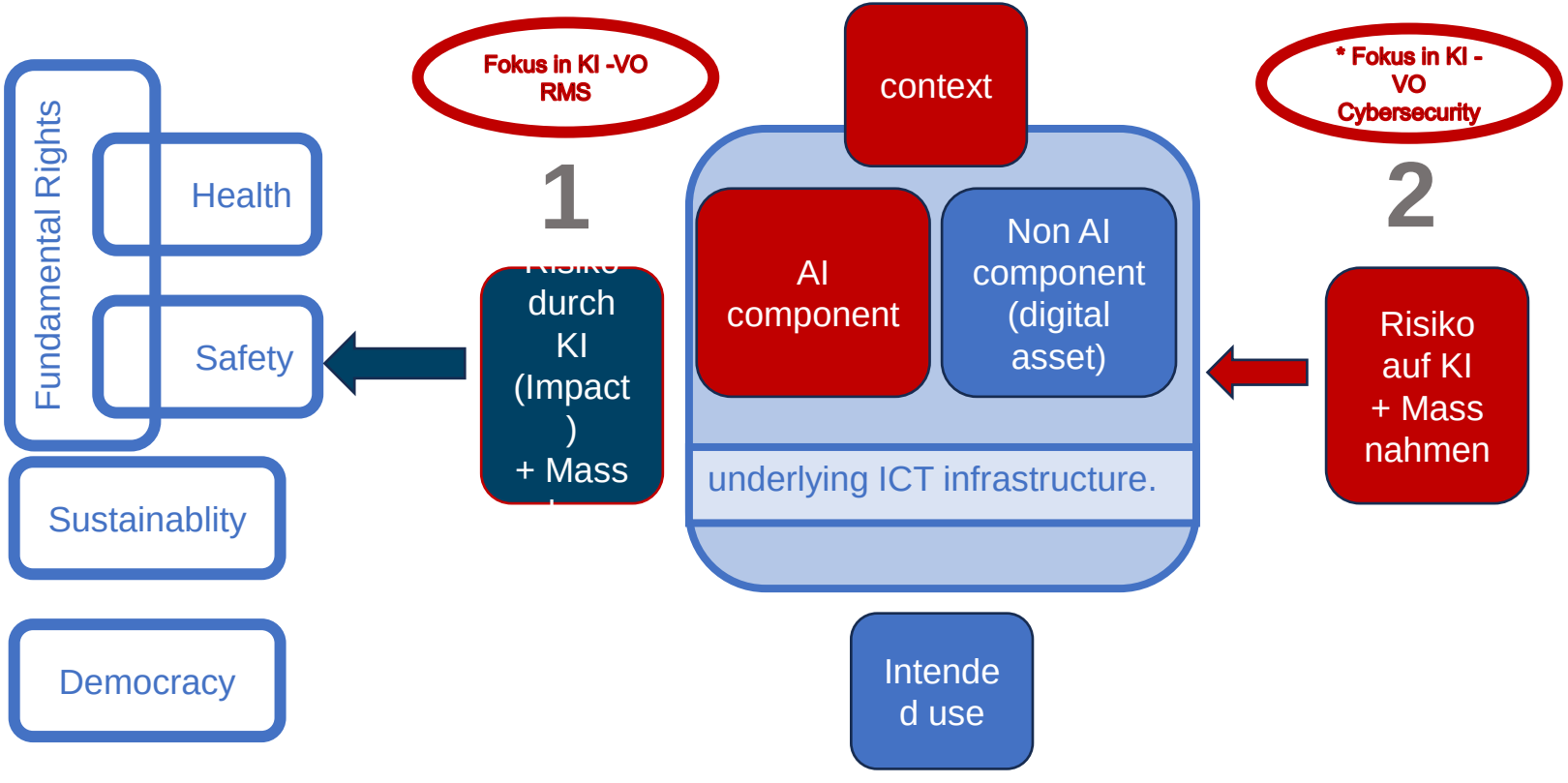
- Hochrisiko-KI-Systeme müssen getestet werden, um die am besten geeigneten gezielten Risikomanagementmaßnahmen zu ermitteln

u.a.m.

Risikomanagement Art.9



Risikomanagement Art.9



Womit kann man heute anfangen ?

- **Überprüfen, ob das geplante KI –System unter Hochrisiko fällt**

a) Es gibt ein Risikomanagementsystem (RMS)

- Überprüfen, einsetzen des RMS für die Schutzziele: Gesundheit, Safety und Grundrechte,
- Überprüfen, ob das vorhandene RMS die Anforderungen aus dem Art. 9 erfüllt, ggfs ergänzen,
- Teilnahme an der Entwurfsumfrage um den Entwurf kennenzulernen

b) Es gibt kein Risikomanagement

- Dringend mit diesem Thema beschäftigen, da nicht nur die KI Verordnung risikobasiert ist
- z.B. BSI Kapitel 7: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_node.html
- z.B. ISO/IEC 31000; 23894; 27005; IEC 62443;

- **Tests zur Überprüfung der Risiko-Minimierungs-Massnahmen**

Qualitätsmanagement (QMS) (Art.17)

Qualitätsmanagementsystem zur Einhaltung der Verordnung, das mit systematisch, ordnungsgemäß **schriftlicher Regeln, Verfahren und Anweisungen** dokumentiert für

- Entwurf, die Entwurfskontrolle und die Entwurfsprüfung des Hochrisiko-KI-System,
- Entwicklung, Qualitätskontrolle und Qualitätssicherung,
- Untersuchungs-, Test- und Validierungsverfahren,
- die technischen Spezifikationen und Normen, die anzuwenden sind
- Systeme und Verfahren für das Datenmanagement
- das in Artikel 9 genannte Risikomanagementsystem
- Einrichtung, Anwendung und Aufrechterhaltung eines Systems zur Beobachtung
- Verfahren zur Meldung und Kommunikation,
- Dokumentation und Ressourcenmanagement

Qualitätsmanagement prEN 18286

Quality management system
- Identifying regulatory requirements
- Determining the scope of the quality management system
- Strategy for regulatory compliance
- Documented information

Management responsibility

Planning

Support (Ressoucen, Kompetenz, Kommunikation)

Product realization

Operation and control incl. Postmarketing Monitoring

Performance evaluation

Womit kann man heute anfangen ?

a) Es ist schon ein Qualitätsmanagement vorhanden

- Überprüfen, ob die Themen aus der KI Verordnung bereits vorhanden sind?
- Ergänzen der Anforderungen aus der KI Verordnung

b) Es ist noch kein Qualitätsmanagement vorhanden

- Dringend mit diesem Thema beschäftigen

Beispiele ISO/IEC
9001 (Qualität),
42001 (AI)
27001 (Security),
14001 (Umwelt),
50001 (Energiemanagement),
45001 (Arbeitsschutz)

Cybersecurity Art.15 (5)

Hochrisiko-KI-Systeme müssen **widerstandsfähig gegen Versuche unbefugter Dritter** sein, ihre Verwendung, Ausgaben oder Leistung **durch Ausnutzung von Systemschwachstellen** zu verändern.
Die technischen Lösungen zur Gewährleistung der Cybersicherheit von Hochrisiko-KI-Systemen müssen den **jeweiligen Umständen und Risiken** angemessen sein.

Die **technischen Lösungen für** den Umgang mit **KI-spezifischen Schwachstellen** umfassen gegebenenfalls **Maßnahmen**, **um Angriffe,** mit denen versucht wird,

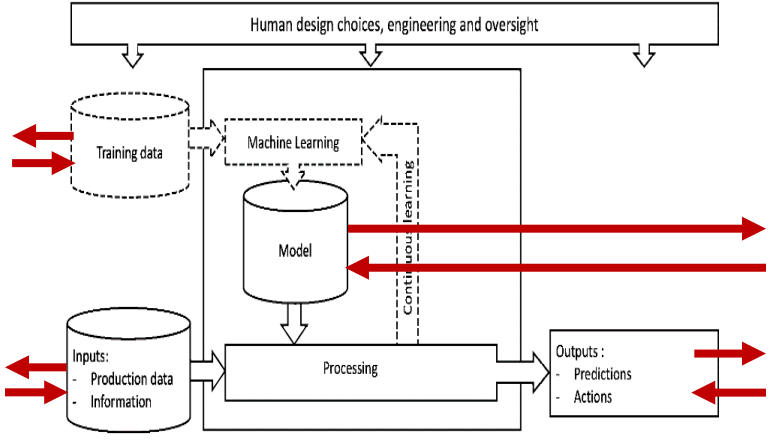
- eine Manipulation des Trainingsdatensatzes **(„data poisoning“)** oder vortrainierter Komponenten, die beim Training verwendet werden (**„model poisoning“)**vorzunehmen,
- Eingabedaten, die das KI-Modell zu Fehlern verleiten sollen **(„adversarial examples“ oder „model evasions**“),
- **Angriffe auf vertrauliche Daten** oder
- **Modellmängel**

zu verhüten, zu erkennen, **darauf zu reagieren, sie zu beseitigen und zu kontrollieren**.

Mögliche Angriffsvektoren speziell bei Maschine Learning AI

Manipulation des Trainingsdatensatzes („data poisoning“)

Eingabedaten, die das KI-Modell zu Fehlern verleiten sollen („adversarial examples“ oder „model evasions“)



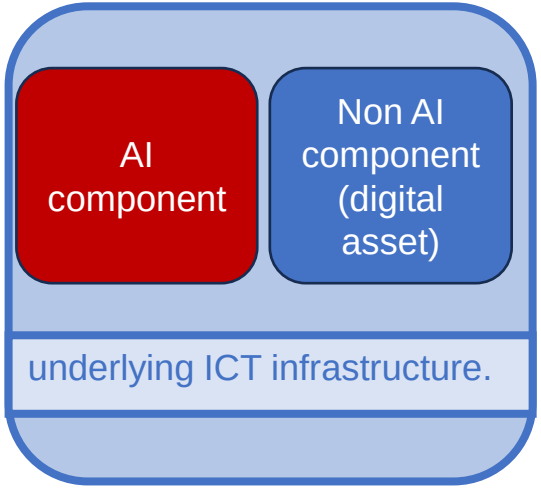
Definition ISO/IEC 22989

Modelmängel, manipuliertes Model („model poisoning“)

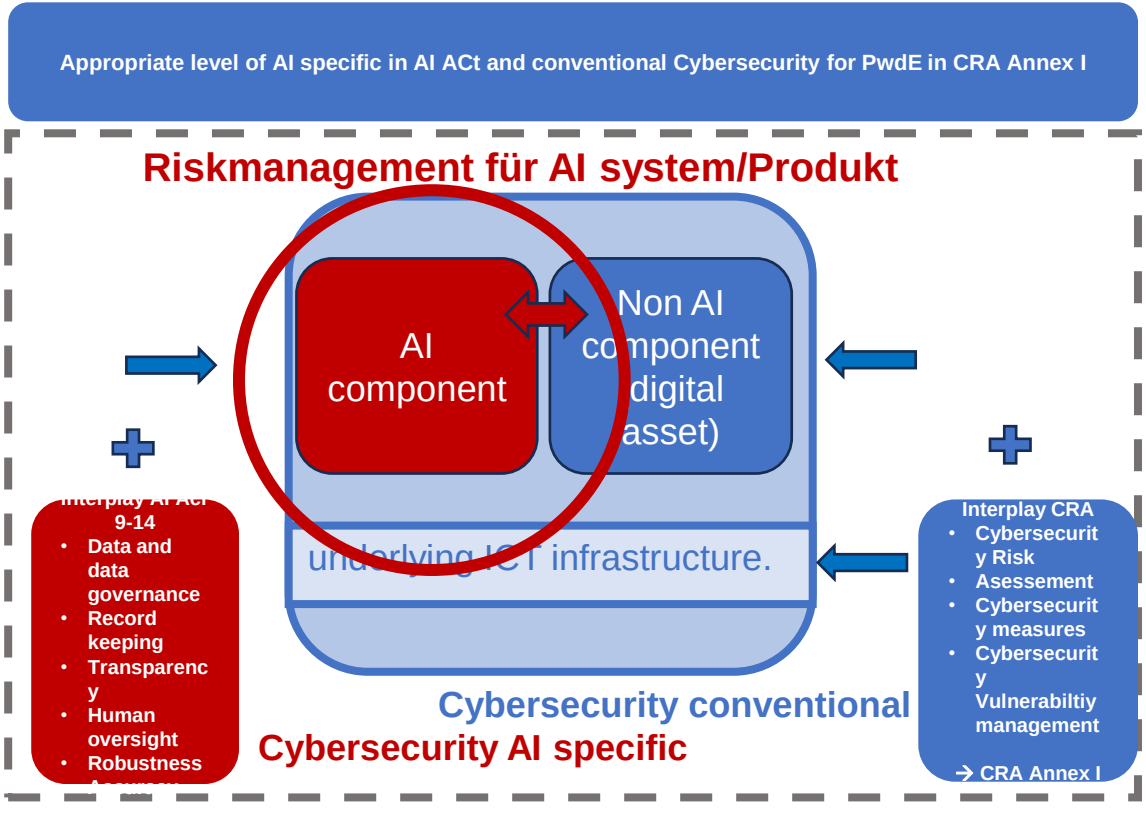
Manipulation der Ausgabedaten

Angriffe auf Vertraulichkeit, Integrität und Verfügbarkeit der Daten, des Model und des gesamten AI-Systems

Cybersecurity- nicht nur für das KI Modell



KI Verordnung und Cyber Resilient Verordnung



* Fokus prEN 18282

AI Act erwartet Resilienz für Produkte mit digitalen Elementen (PwdE) + AI

und einen angemessenen Level von Cybersecurity über den Lebenslauf.

Womit kann man heute anfangen?

Cyber Resilience Act und geplante Standards ansehen

a) Es ist ein Cybersecurity Management vorhanden

- Überprüfen wie ein KI-Systems mit den Anforderungen aus Art. 15 (5) integriert werden kann

b) Es ist kein Cybersecurity Management vorhanden

- Dringend mit diesem Thema beschäftigen

Beispiele:

- Bundesamt für Sicherheit in der Informationstechnik : BSI Grundschutz
- ISO/IEC 27001/ 27002
- IEC 62443

Zusammenfassung

KI Verordnung hat das Ziel Gesundheit, Sicherheit und die Grundrechte vor Hochrisiko KI Systemen zu schützen

Die Nutzung harmonisierter Standards (Normen) gilt automatisch als Nachweis

10 Standards wurden in Auftrag geben – Fertigstellung geplant für Ende 2026

Unbedingt heute anfangen , z.B. mit

- Qualitätsmanagement und Dokumentation
- Risikomanagement
- Cybersecurity Management
- Datenmanagement
- Menschliche Aufsicht

Viel Erfolg

Annegrit Seyerlein-Klug

- Dipl. Ing. (Maschinenbau, Medizintechnik)
- M.Sc. Security Management; M.Sc. Technologie und Innovation

- ISO 27001 und ITIL zertifiziert
- Nixdorf; Siemens Nixdorf/ Siemens Business Services, Siemens/Siemens Enterprise/Unify; Secunet (Security KRITIS); Neurocat (AI Security and Robustness); Intcube (AI Security)
- Technische Hochschule Brandenburg

  - **DIN/CEN/ISO IT/Cybersecurity und KI**

  - **Convenor CEN/CENELEC JTC 21 WG5**
    Cybersecurity Specification for AI-systems

annegrit.seyerleinklug@th-brandenburg.de

Informationen und Mitwirkungsmöglichkeit im Überblick

- DIN Normungs-Monitor: Hilfreiche Übersicht über aktuelle und zukünftige Normungsvorhaben, Entwurfsveröffentlichungen sowie Rücknahmen von Normen an.

- Norm-Entwurfs-Portal: Möglichkeit zur Kommentierung von Norm-Entwürfen um aktiv an der Entwicklung mitzuwirken.

- Mitwirkungsmöglichkeiten:
  - **Mitarbeit im nationalen Spiegelgremium**, um alle Dokumente und Arbeitsentwürfe einsehen und ggf. kommentieren zu können
  - **Entsendung in die europäischen und internationalen Gremien**, um direkt an der Entwicklung mitzuwirken
  - Experten können den Prozess der Entwicklung einer Norm leiten, indem sie **Projektleiter/"Editor"** werden

Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen oder weiterem Interesse melden Sie sich gerne unter:
Digitalisierung_KMU@BNetzA.DE

Hier finden Sie außerdem den Link zur **Anlaufstellendatenbank**:

https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/Mittelstand/Anlaufstellen/start.html