

Die Umsetzung der KI-Verordnung: Weg zur Compliance und Chance für Qualität

Infoveranstaltung IHK Hessen / digitales.hessen

Dr. Sebastian Hallensleben

Chair CEN-CENELEC JTC21
Chief Trust Officer, Resaro
Co-Chair AI Risk & Accountability OECD ONE.AI
Programme Chair, Digital Trust Convention
Principal Advisor Digital Trust, KI Park



2025-09-03

www.linkedin.com/in/sebastianhallensleben

sebastian@hallensleben.org



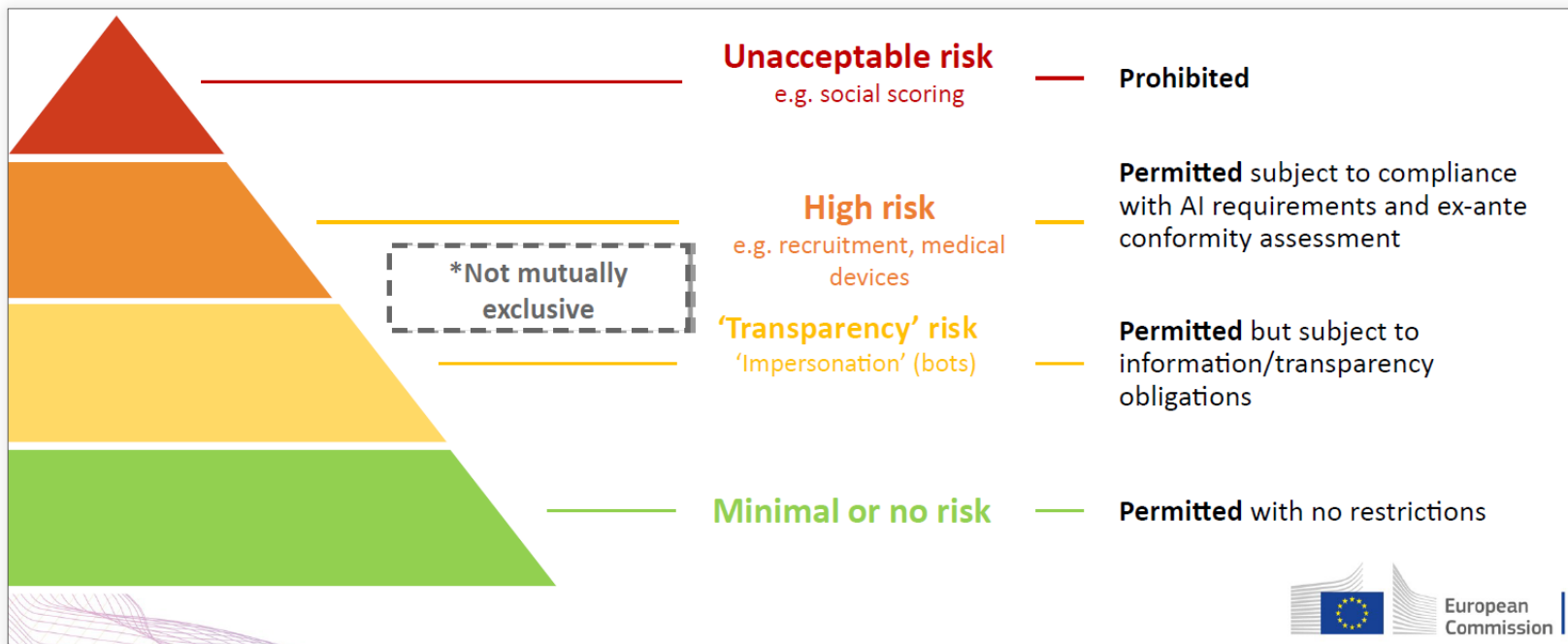
Harmonisierte Standards:

Der rechtssichere Weg zur Compliance mit der KI-Verordnung

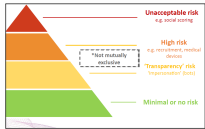
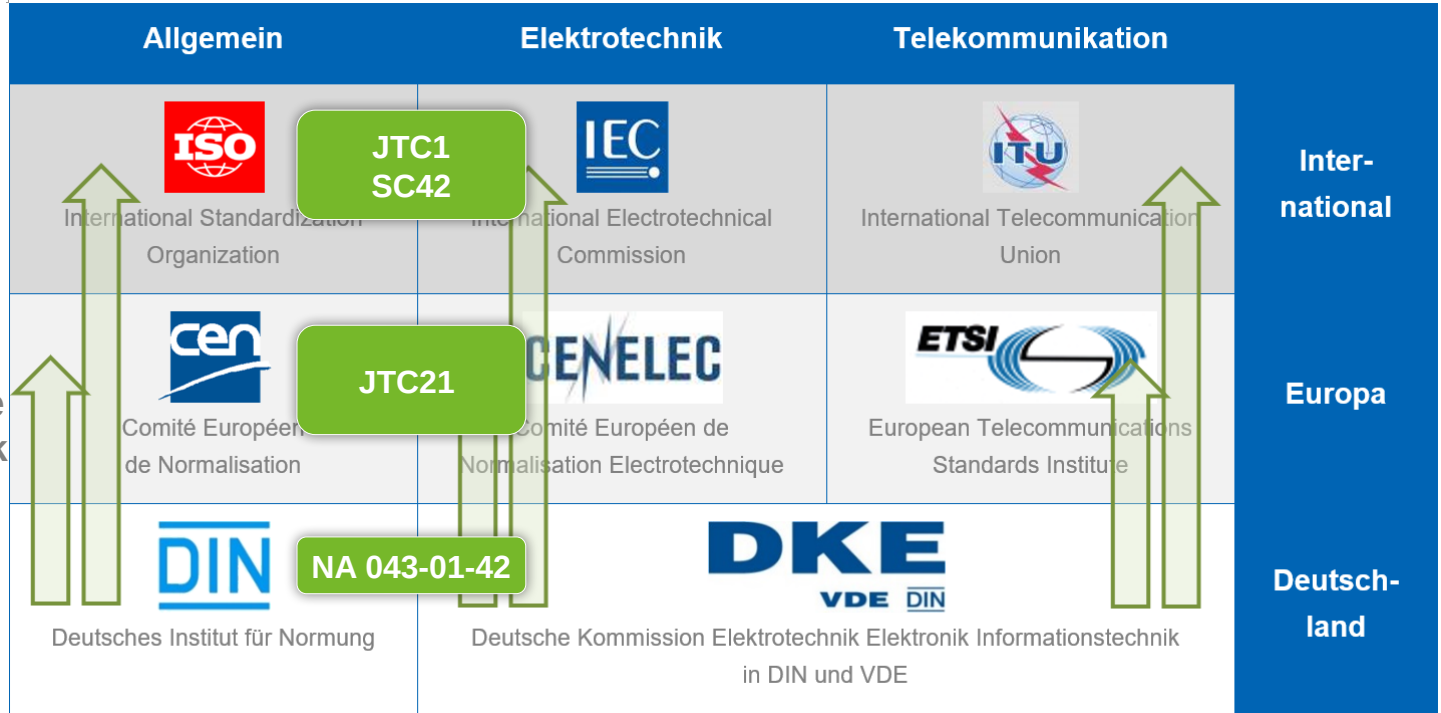


Anforderungen im EU AI Act:

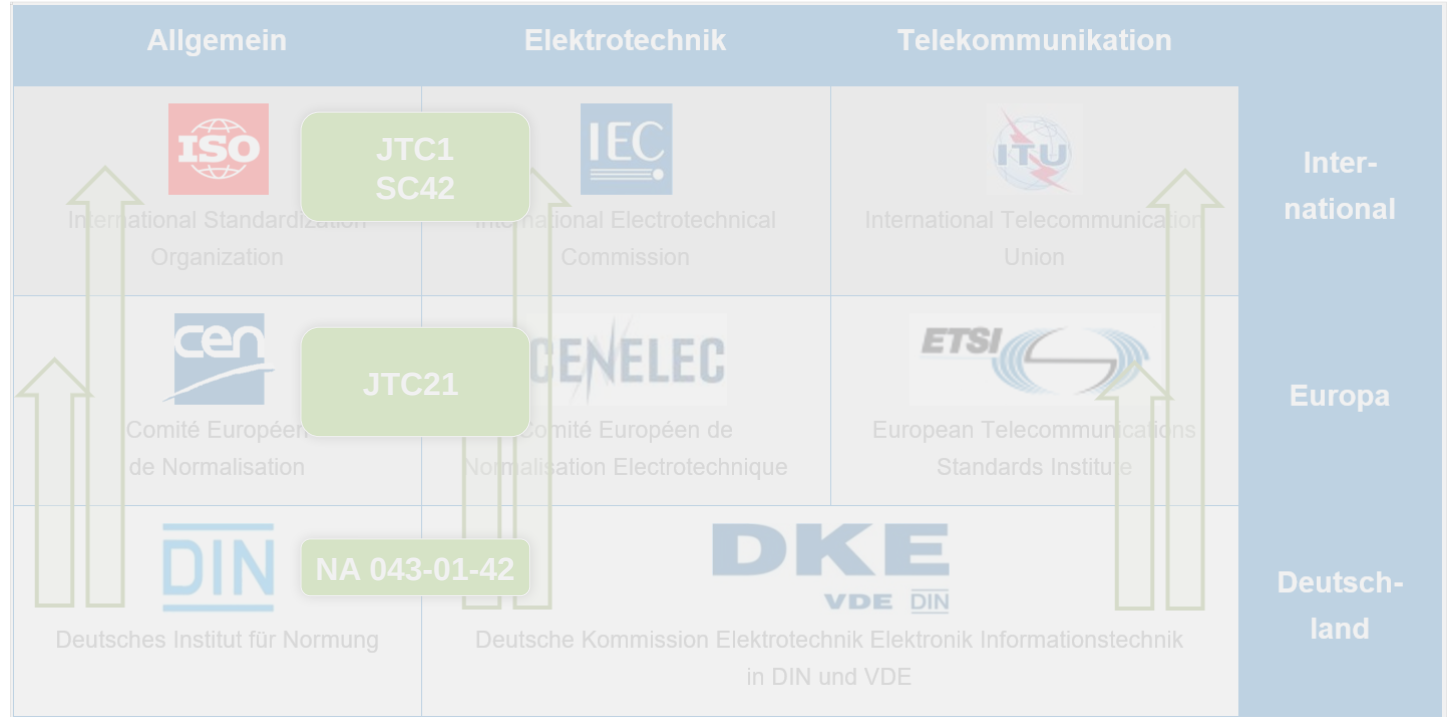
Nur grobe Anforderungen ⇒ Details werden woanders definiert



Globale Struktur der Normung / Standardisierung



Synergie von Regulierung und Standardisierung



Synergie von Regulierung und Standardisierung



Standardisierungsmandat der EU

1.	European standard(s) and/or European standardisation deliverable(s) on risk management system for AI systems
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems
3.	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems
4.	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions to the users of AI systems
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems

6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems
9.	European standard(s) and/or European standardisation deliverable(s) on quality management system for providers of AI systems, including post-market monitoring process
10.	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems

[illegible]

Zur ISO/IEC 42001: Management System Standard for AI

- Veröffentlicht November 2023
- Welle an Beratungs- und Prüfungsangeboten weltweit

Warum übernehmen wir die 42001 nicht einfach für Europa?

Klares und frühzeitiges „Nein“ der EU wegen mehrfachem Mismatch:

42001	Bedarf für AI Act
Risikoverständnis nach ISO 31000 / Guide 73: Risiko = Unsicherheit	Risikoverständnis nach IEC Guide 51: Risiko = Schaden x Eintrittswahrscheinlichkeit
Bezieht sich auf eine Organisation	Bezieht sich auf ein Produkt
Fokus auf Good Practice	Fokus auf messbaren, durchsetzbaren Anforderungen



Vorgehen im JTC21:

Europaspezifische Standards für Qualitäts- und Risikomanagement, aber mit starker Referenzierung von 42001, 14791 etc.

JTC21 Working Groups

- WG1: Strategic Advisory Group
- WG2: Operational Aspects
- WG3: Engineering Aspects
- WG4: Foundational and Societal Aspects
- WG5: Cybersecurity

(in collaboration with ETSI, ENISA and CEN-CENELEC JTC13)

~200 Experten direkt im JTC21
~25 Länder
>1000 Experten nationale Ebene

Rekordgröße wegen -

- Breite der Stakeholder und Interessen
- Breite der Anwendungsgebiete
- KI ist heißes Thema



Standardisierung liefert zwei Ergebnisse

- **Sichtbar:**
ein Satz von aufeinander abgestimmten **technischen Standards**
- **Unsichtbar:**
Konsens “aller interessierten Kreise” (=> **Legitimität**)

Risiken und deren Mitigierung

Risiken / Herausforderungen	Mitigierung
Endliche Bandbreite in der europäischen Normung	▪ Aufbau auf internationale Standards wo immer möglich ▪ Direct adoption, wo ausreichend ▪ Modified adoption als innovativer Prozess, von CEN-CENELEC bestätigt
Verzögerungen und inhaltliche Unwägbarkeiten in der internationalen Normung	▪ Sparsame Verwendung von „parallel development“ ▪ Adoption nur, wenn intl. Standard bereits (fast) fertiggestellt, d.h. inhaltlich und zeitlich stabil sind
Hoher Anspruch des AI Acts; Interpretationsspielräume; HAS Assessment	▪ Aktive Rolle der EU-Kommission (DG CNECT) in JTC21 bei Plenary Meetings sowie in den Arbeitsgruppen schon seit 2021 ⇒ frühzeitige Ausräumung von Unsicherheiten und Kontroversen ▪ Verzicht auf den HAS-Prozess, stattdessen direkte Beurteilung durch DG CNECT
z.T. schwierige Konsensbildung durch divergierende Interessen	▪ Regelmäßige Bereitstellung von Analysen durch den Joint Research Council ▪ Intensive politische Unterstützung und Flankierung durch die EU-Kommission ▪ Verdeutlichung der allseits unerfreulichen Auswirkungen von „common specifications“ ▪ Straffung von CEN-CENELEC-Prozessen ⇒ mehr Zeit für inhaltliches Alignment

Timeline

- CEN-CENELEC: AI Focus Group seit **2019** | JTC21 seit **2021**
- AI Act **final** seit August 2024
- Stocktaking Review durch KOM / AI Office **Feb 2025**
=> gemeinsames Verständnis der noch zu schließenden Lücken
- Öffentliche Konsultation zu den Entwürfen der harmonisierten Standards („**Enquiry Vote**“) v.a. in **Q4 / 2025**
- Einarbeitung des Feedbacks („**Comment Resolution**“) v.a. in **Q1 / 2026** => inhaltliche Reife
- Deadline Umsetzung high-risk requirements **Aug 2026** (?)
- Formale Prozesse in CEN-CENELEC sowie KOM / AI Office für Finalisierung, Harmonisierung und OJEU-Veröffentlichung



JTC21 standards are currently distinct from the Code of Practice

	JTC21 harmonised standards	Code of Practice
Providing implementation steps for ...	Requirements on AI systems in high-risk applications – Articles 8 to 15 • All types of AI • Late stage of value chain	Requirements on General Purpose Models – Articles 53, 55 • Generative AI only • Early stage of value chain
Development context and process	• Broadly applicable complex set of CEN-CENELEC regulations • Decision making power with standardisation bodies at national level who also provide secretarial support (~25 countries) • Input from ETSI (under Mode 4) • Input from ISO/IEC (under Vienna/Frankfurt agreements) • Ongoing feedback/guidance from EC at working level	• Custom process and structure created for CoP development purposes • Process directed by AI Office with outsourced facilitation support • Decision making power is with the AI Office

Initiation of a standardisation request based on the CoP expected for H2/2025.

Compliance und Qualität: Zwei Fliegen mit einer Klappe schlagen





[https://commons.wikimedia.org/wiki/File:Geneva_International_Motor_Show_2018_Le_Grand-Saconnex_\(1X7A0036\).jpg](https://commons.wikimedia.org/wiki/File:Geneva_International_Motor_Show_2018_Le_Grand-Saconnex_(1X7A0036).jpg)

Qualität potenzieller KI-Lösungen klar beschreiben

- Wann ist eine KI-Lösung **“gut genug”** für den Einsatz?
- Wie lässt sich **”gut genug”** (= ein gewünschtes Qualitätsniveau) beschreiben?
- Woran lässt sich festmachen,
ob Lösung X **besser oder schlechter** ist als Lösung Y?
(→ Anbietervergleich; Entscheidung make vs. buy)

Erfüllung von Regularien
ist kein Qualitätsmerkmal,
sondern wird
selbstverständlich
vorausgesetzt

AI Solution Quality Index (Resaro ASQI)

als gemeinsame Sprache
von Fachbereichen,
Governance und Technik

für alle anvisierten
KI-Use-Cases in
einer Organisation



Fazit:

1. **Harmonisierte Standards sind der rechtssichere Weg zur Compliance mit der KI-Verordnung**
2. **Haben Sie auch bei KI-Systemen den Mut, handfeste Qualität zu verlangen!**
3. **Packen Sie Compliance und Qualität gemeinsam an.**

