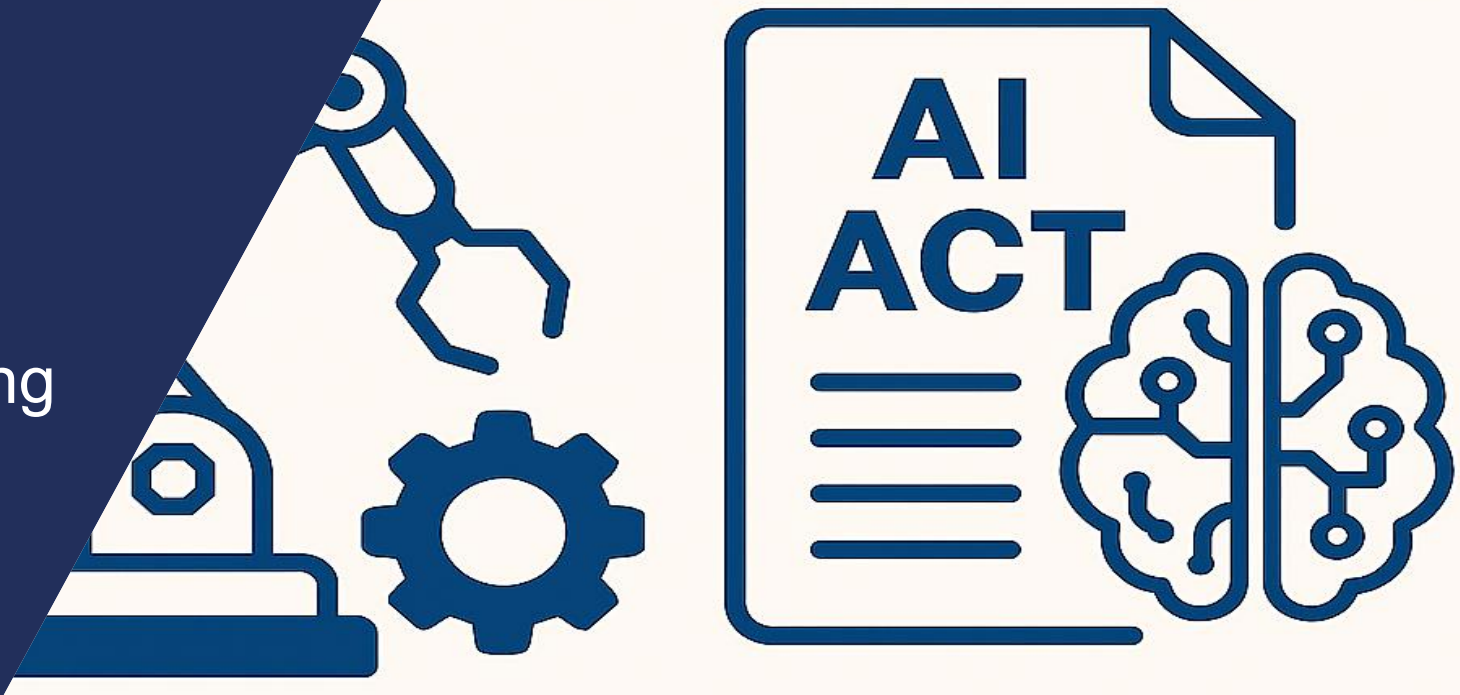
VDMA

ABTEILUNG TECHNIKPOLITIK UND STANDARDISIERUNG

FACHVERANSTALTUNG MASCHINENSICHERHEIT

Regulierte Intelligenz: Anforderungen an KI gemäß der Maschinen- und der KI-Verordnung



23.09.2025

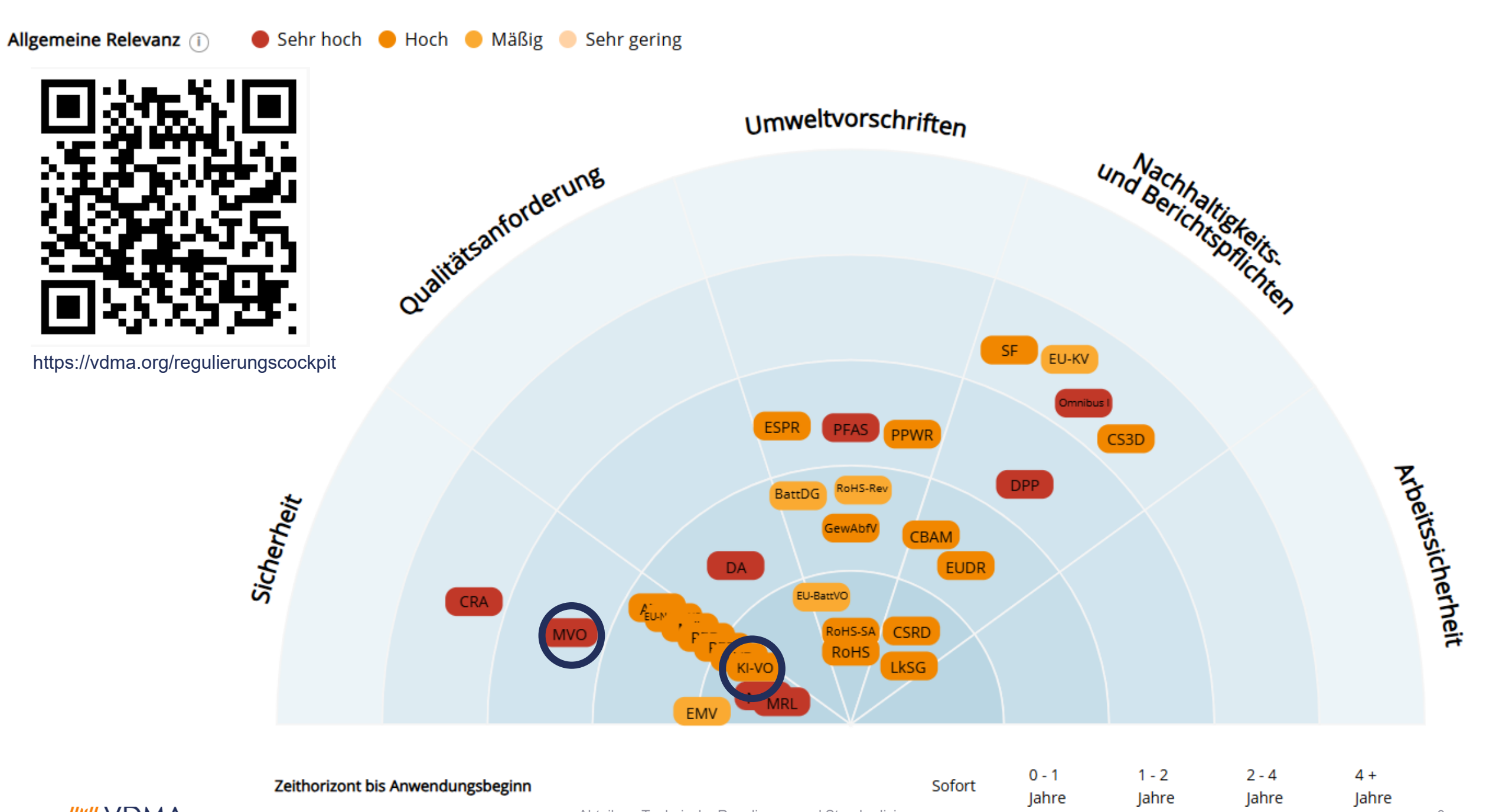
DR. JACOB L. GORENFLOS LÓPEZ

REFERENT FÜR TECHNISCHE REGULIERUNG

ADVANCING EUROPE'S MACHINERY INDUSTRY

Das wichtige steht im gelb markierten Text

Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Das wichtige steht im gelb markierten Text
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla
Bla bla bla bla bla bla bla



https://vdma.org/regulierungscockpit

Agenda

01 **WARUM SOLLTEN WIR UNS MIT KI REGULIERUNG BESCHÄFTIGEN?**

02 **WAS SAGT DIE MVO ZU KI?**

UND

WIE FUNKTIONIERT DIE KI-VO?

03 **STAND DER KI-NORMUNG FÜR DIE KI-VO**

Warum sollten wir uns mit KI Regulierung Beschäftigen?

Zeitschiene des Inkrafttretens von KI Regulierenden Gesetzen

02.02.2025
2024/1689
Verbotene Praktiken

2023/1230 Maschinenverordnung
2024/1689 KI-Verordnung

Verbotene Praktiken | Art. 5

- **Unterschwellige Beeinflussung oder Täuschung** mit dem Ziel, Verhalten wesentlich zu verändern und dadurch erheblichen Schaden zu verursachen.
- **Ausnutzung von Schutzbedürftigkeit** (z. B. Alter, Behinderung, soziale Lage) zur Verhaltensbeeinflussung mit möglichem erheblichen Schaden.
- **Soziale Bewertung (Social Scoring)** zur Benachteiligung in sozialen Kontexten oder in ungerechtfertigter Weise.
- **Risikobewertung zur Vorhersage kriminellen Verhaltens** ausschließlich durch Profiling oder persönliche Merkmale, ohne objektive Tatsachenbasis.
- **Gesichtserkennungsdatenbanken** aus Internetbildern oder Überwachung zur Erstellung/Erweiterung.
- **Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen**, außer bei medizinischer oder sicherheitsbezogener Begründung.
- **Biometrische Kategorisierung** zur Ableitung sensibler Merkmale (z. B. Rasse, Religion, sexuelle Orientierung).
- **Biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum zu Strafverfolgungszwecken**, außer in klar geregelten Ausnahmefällen:
    - Suche nach Opfern oder vermissten Personen.
    - Abwendung konkreter Gefahren (z. B. Terroranschlag).
    - Identifizierung von Verdächtigen schwerer Straftaten.

Verbotene Praktiken | KI-Verordnung Art. 5

- **Unterschwellige Beeinflussung oder Täuschung** mit dem Ziel, Verhalten wesentlich zu verändern und dadurch erheblichen Schaden zu verursachen.
- **Ausnutzung von Schutzbedürftigkeit** (z. B. Alter, Behinderung, soziale Lage) zur Verhaltensbeeinflussung mit möglichem erheblichen Schaden.
- **Soziale Bewertung (Social Scoring)** zur Benachteiligung in sozialen Kontexten oder in ungerechtfertigter Weise.
- **Risikobewertung zur Vorhersage kriminellen Verhaltens** ausschließlich durch Profiling oder persönliche Merkmale, ohne objektive Tatsachenbasis.
- **Gesichtserkennungsdatenbanken** aus Internetbildern oder Überwachung zur Erstellung/Erweiterung.
- **Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen**, außer bei medizinischer oder sicherheitsbezogener Begründung.
- **Biometrische Kategorisierung** zur Ableitung sensibler Merkmale (z. B. Rasse, Religion, sexuelle Orientierung).
- **Biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum zu Strafverfolgungszwecken**, außer in klar geregelten Ausnahmefällen:
    - Suche nach Opfern oder vermissten Personen.
    - Abwendung konkreter Gefahren (z. B. Terroranschlag).
    - Identifizierung von Verdächtigen schwerer Straftaten.

Zeitschiene des Inkrafttretens von KI Regulierenden Gesetzen

2023/1230 Maschinenverordnung
2024/1689 KI-Verordnung

Was sagt die MVO zu KI?

Was sagt die MVO zu KI?

Wenn KI Sicherheitsfunktionen (selbstentwickelnd; Ansätzen des maschinellen Lernens) im Sicherheitsbauteil übernimmt, dann Drittstellenprüfung

Was steht im Text der MVO zu KI?

KONFORMITÄTSBEWERTUNG
Artikel 25
Konformitätsbewertungsverfahren für Maschinen und dazugehörige Produkte
(1) Der Hersteller oder die in Artikel 18 genannte natürliche oder juristische Person wendet eines der in den Absätzen 2, 3 und 4 beschriebenen Konformitätsbewertungsverfahren an.
(2) Ist die Kategorie von Maschinen oder dazugehörigen Produkten in Anhang I Teil A aufgeführt, so wendet der Hersteller oder die in Artikel 18 genannte natürliche oder juristische Person eines der folgenden Verfahren an:

a) EU-Baumusterprüfung (Modul B) gemäß Anhang VII, gefolgt von der Konformität mit dem Baumuster auf der Grundlage einer internen Fertigungskontrolle (Modul C) gemäß Anhang VIII;

b) Konformität auf der Grundlage einer umfassenden Qualitätssicherung (Modul H) gemäß Anhang IX;

c) Konformität auf der Grundlage einer Einzelprüfung (Modul G) gemäß Anhang X.

Erfordern Drittstelle

ANHANG I

KATEGORIEN VON MASCHINEN ODER DAZUGEHÖRIGEN PRODUKTEN, AUF DIE EINES DER IN ARTIKEL 25 ABSÄTZE 2 UND 3 GENANNTEN VERFAHREN ANZUWENDEN IST

TEIL A

Kategorien von Maschinen oder dazugehörigen Produkten, auf die ein in Artikel 25 Absatz 2 genanntes Verfahren anzuwenden ist:

[…]

5. Sicherheitsbauteile mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens, die Sicherheitsfunktionen gewährleisten.

6. Maschinen, die über eingebettete Systeme mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens verfügen, die Sicherheitsfunktionen gewährleisten, die nicht gesondert in Verkehr gebracht wurden, nur in Bezug auf diese Systeme.

Was sagt die Maschinenverordnung zu KI?

(55)

Die Bestimmungen dieser Verordnung über die Konformitätsbewertung von Software, die Sicherheitsfunktionen gewährleistet, durch unabhängige Dritte sollten nur für Systeme mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens, die Sicherheitsfunktionen gewährleisten, gelten. Dagegen sollten diese Bestimmungen **nicht für Software gelten, die weder lern- noch weiterentwicklungsfähig ist** und nur für die **Ausführung bestimmter automatisierter Funktionen** von Maschinen oder dazugehörigen Produkten programmiert ist.

Bitte wie ein Jurist denken

„weder lern- noch weiterentwicklungsfähig ist“

„Ausführung bestimmter automatisierter Funktionen“

MVO und KI-VO Guide klärt, evtl.?

„lern- und weiterentwicklungsfähig ist“

„Ausführung nicht finit definiert automatisierter Funktionen“

Verschiedenste Abstufungen zwischen diesen „Extremen“ sind denkbar.

Grundlagen der KI-VO

KI-VO: Ein risikobasierter Ansatz

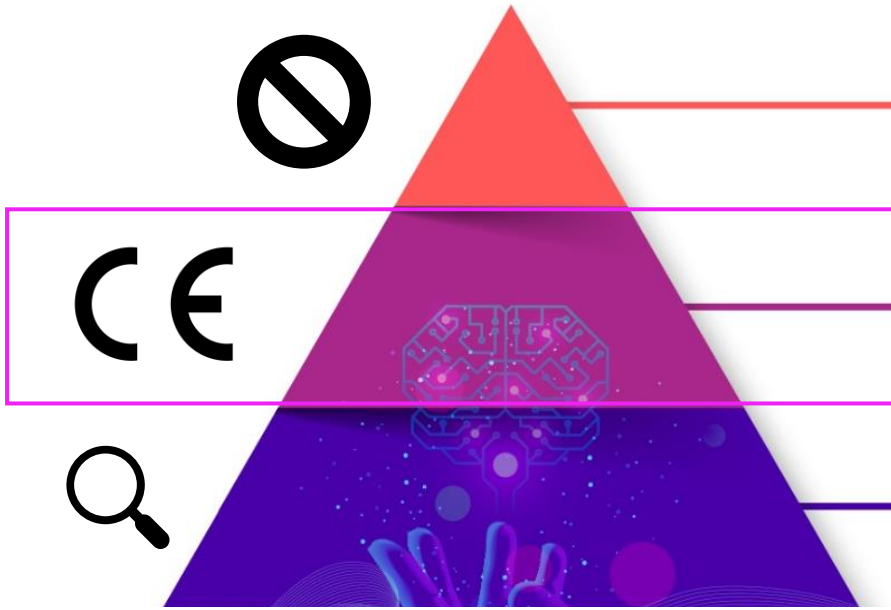
Inakzeptables Risiko

CE

Hohes Risiko

Zentrale Fokus

KI-VO: Ein risikobasierter Ansatz



Inakzeptables Risiko

Hohes Risiko

Zentrale Fokus

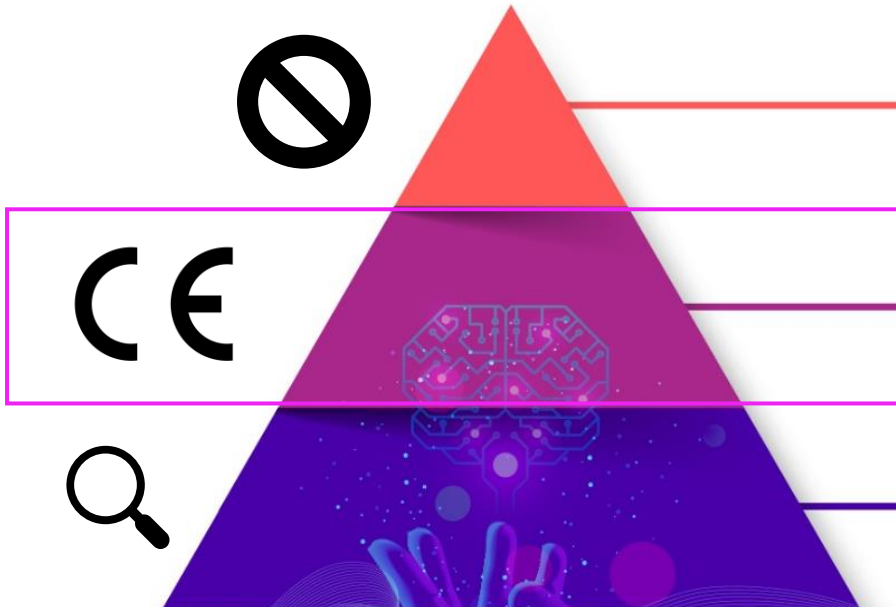
Begrenztes Risiko

Erlaubt, aber mit Informations-/Transparenzpflichten verbunden (z.B. Information, dass es sich um AI handelt)

Transparenzpflichten | Art. 50

Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, müssen offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde. Diese Pflicht gilt nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen ist oder wenn die durch KI erzeugten Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt.

KI-VO: Ein risikobasierter Ansatz



Inakzeptables Risiko

Hohes Risiko

Zentrale Fokus

Begrenztes Risiko

Erlaubt, aber mit Informations-/Transparenzpflichten verbunden (z.B. Information, dass es sich um AI handelt)

PLUS: Systemisches Risiko durch „general-purpose AI", insb. große generative KI Modele

Zentrale Wirtschaftsakteure in der KI-Verordnung

Pendant aus der Maschinenverordnung ist in der Regel der Hersteller

Weitere Wirtschaftsakteure:
- **Bevollmächtigter der Anbieter (Art. 22)**
- **Einführer (Art. 23)**
- **Händler (Art. 24)**
- Für Verantwortlichkeiten entlang der Wertschöpfungskette siehe Art. 25

Zentrale Wirtschaftsakteure in der KI-Verordnung

Pendant aus der Maschinenverordnung ist in der Regel der Hersteller

Weitere Wirtschaftsakteure:
- **Bevollmächtigter der Anbieter (Art. 22)**
- **Einführer (Art. 23)**
- **Händler (Art. 24)**
- Für Verantwortlichkeiten entlang der Wertschöpfungskette siehe Art. 25

Pflichten der Betreiber von Hochrisiko-KI-Systemen | Art. 26

- **Ordnungsgemäße Nutzung**: Betrieb nach Anleitung und Vorschriften
- **Menschliche Aufsicht**: nur kompetentes, geschultes Personal einsetzen
- **Qualität der Eing**
- **Überwac**
- **Proto**
- **Inform**
- **Registrierung**
- **Datenschutz**: ggf. Folgenabsch
- **Kooperation**: mit Aufsichtsbehörden zusammenarbeiten

Checkliste für VDMA Unternehmen aktuell in Arbeit

Wann wird meine KI zur Hoch-Risiko-KI?

KI-VO Anforderungen an Hoch-Risiko-KI (Art. 16)

- Drittstelle für Teil der Prüfung (Art. 6)

- **Kapitel III Abschnitt 2**
- Risikomanagementsystem (Art. 9)
- Daten und Daten-Governance (Art. 10)
- Technische Dokumentation (Art. 11)
- Aufzeichnungspflichten (Art. 12)
- Transparenz und Bereitstellung von Informationen für die Betreiber (Art. 13)
- Menschliche Aufsicht (Art. 14)
- Genauigkeit, Robustheit und Cybersicherheit (Art. 15)

- **Kapitel III Abschnitt 3**
- Qualitätsmanagementsystem (Art. 17)
- Aufbewahrung der Dokumentation (Art. 18)
- Automatisch erzeugte Protokolle (Art. 19)
- Korrekturmaßnahmen und Informationspflicht (Art. 20)
- Zusammenarbeit mit den zuständigen Behörden (Art. 21)

- **Weitere**
- Konformitätsbewertungsverfahren (Art. 43) und Konformitätserklärung (Art. 47)
- Registrierung (Art. 49 Abs. 1)
- Barrierefreiheitsanforderungen gemäß den Richtlinien (EU) 2016/2102 und (EU) 2019/882

Zentrale Wirtschaftsakteure in der KI-Verordnung

Pendant aus der Maschinenverordnung ist in der Regel der Hersteller

Weitere Wirtschaftsakteure:
- **Bevollmächtigter der Anbieter (Art. 22)**
- **Einführer (Art. 23)**
- **Händler (Art. 24)**
- Für Verantwortlichkeiten entlang der Wertschöpfungskette siehe Art. 25

Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 | Anhang III

1. Biometrie
2. **Kritische Infrastruktur**
3. Allgemeine und berufliche Bildung
4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen
6. Strafverfolgung
7. Migration, Asyl und Grenzkontrolle
8. Rechtspflege und demokratische Prozesse

Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 | Anhang III

Kritische Infrastruktur in Anhang III der KI-VO

„KI-Systeme, die bestimmungsgemäß als Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen“

Definition kritischer gemäß Richtlinie (EU) 2022/2557 Art. 2 Abs. 4

4. „kritische Infrastrukturen“ Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile eines Objekts, einer Anlage, Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind;

5. „wesentlicher Dienst“ einen Dienst, der für die Aufrechterhaltung wichtiger
gesellschaftlicher Funktionen,
wichtiger wirtschaftlicher Tätigkeiten,
der öffentlichen Gesundheit und
Sicherheit oder der Erhaltung der Umwelt von entscheidender Bedeutung ist;

Überlapp KI-VO zu MVO (Teil 1)

Kriterien
1. **Sicherheitsbauteil**
2. **Konformitätsbewertung durch 3.**

KI-Verordnung

Artikel 6

Einstufungsvorschriften für Hochrisiko-KI-Systeme

(1) Ungeachtet dessen, ob ein KI-System unabhängig von den unter den Buchstaben a und b genannten Produkten in Verkehr gebracht oder in Betrieb genommen wird, gilt es als Hochrisiko-KI-System, wenn die beiden folgenden Bedingungen erfüllt sind:

a) das KI-System soll als Sicherheitsbauteil eines unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet werden oder das KI-System ist selbst ein solches Produkt;

b) das Produkt, dessen Sicherheitsbauteil gemäß Buchstabe a das KI-System ist, oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieses Produkts gemäß den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union unterzogen werden.

ANHANG I

Liste der Harmonisierungsrechtsvorschriften der Union
Abschnitt A — Liste der Harmonisierungsrechtsvorschriften der Union auf der Grundlage des neuen Rechtsrahmens

1. Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (ABl. L 157 vom 9.6.2006, S. 24)

Kriterien
1. **Sicherheitsbauteil**
2. **Konformitätsbewertung durch 3.**

Überlapp KI-VO zu MVO (Teil 2)

Was ist ein Sicherheitsbauteil?

KI-Verordnung

Artikel 3

Begriffsbestimmungen

14. „Sicherheitsbauteil“ einen Bestandteil eines Produkts oder KI-Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet;

Maschinen-Verordnung

Artikel 3

Begriffsbestimmungen

3. „Sicherheitsbauteil “ bezeichnet ein physisches oder digitales Bauteil, einschließlich Software, eines in den Anwendungsbereich dieser Verordnung fallenden Produkts, die zur Gewährleistung einer Sicherheitsfunktion konstruiert oder bestimmt ist, gesondert in Verkehr gebracht wird und dessen Ausfall oder Fehlfunktion die Sicherheit von Personen gefährdet, die aber für das Funktionieren dieses Produkts nicht erforderlich ist oder durch normale Bauteile ersetzt werden kann, um den Betrieb dieser Produkte zu gewährleisten;

Kriterien
1. Sicherheitsbauteil
2. Konformitätsbewertung durch 3.

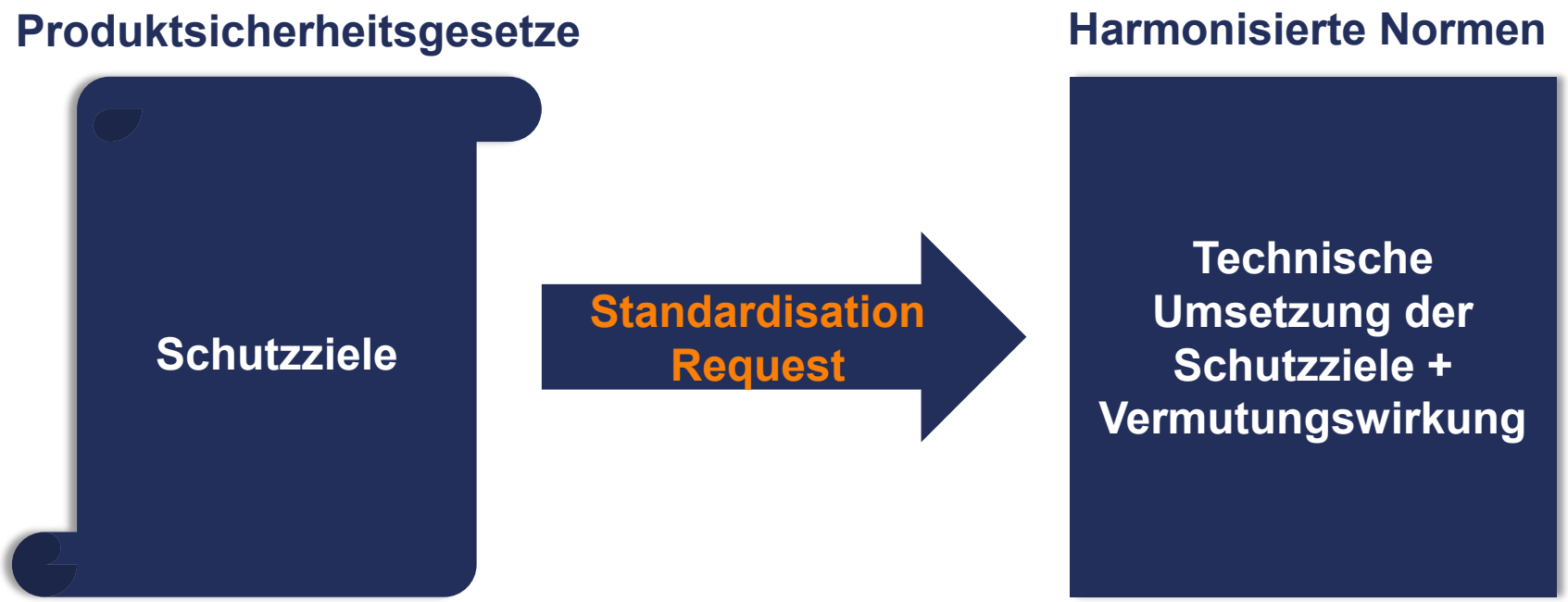
Überlapp KI-VO zu MVO (Teil 3)

Wenn KI Sicherheitsfunktionen (selbstentwickelnd; Ansätzen des maschinellen Lernens) im Sicherheitsbauteil übernimmt, dann Drittstellenprüfung

KI-Normung für die KI-Verordnung

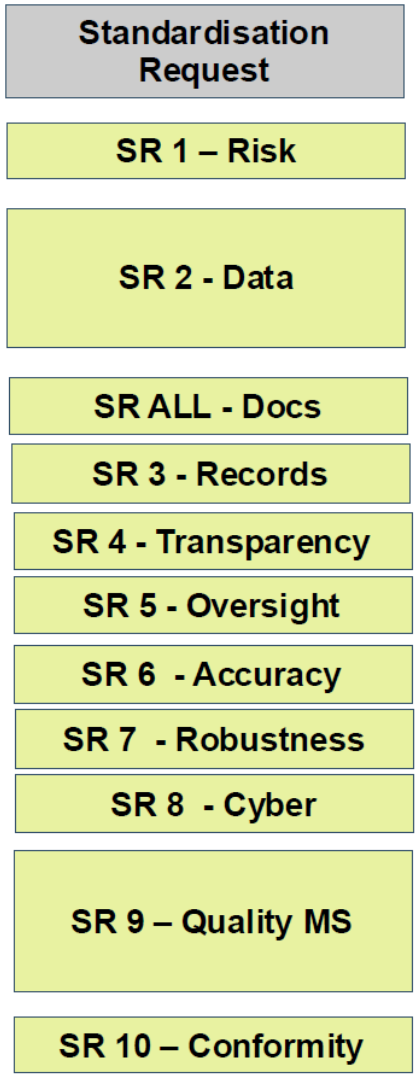
Unterschied zwischen EN und hEN

Alle hEN sind auch EN

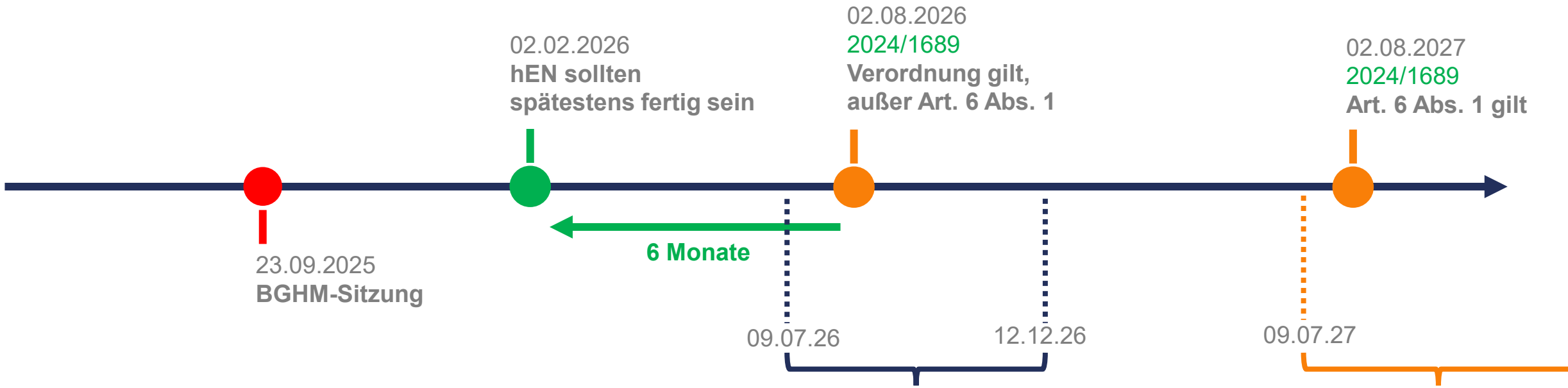


SReq zu KI-VO zu Normungsprojekte

JTC 21 Folie



Wann sollten die hEN fertig sein?



In diesem Zeitraum sollen die meisten hEN laut aktueller Planung fertig werden.

Einschätzung:
Wahrscheinlich wird es sich in den meisten Fällen um mind. 12 Monate verzögern.

2024/1689 KI-Verordnung

VDMA Unterstützung

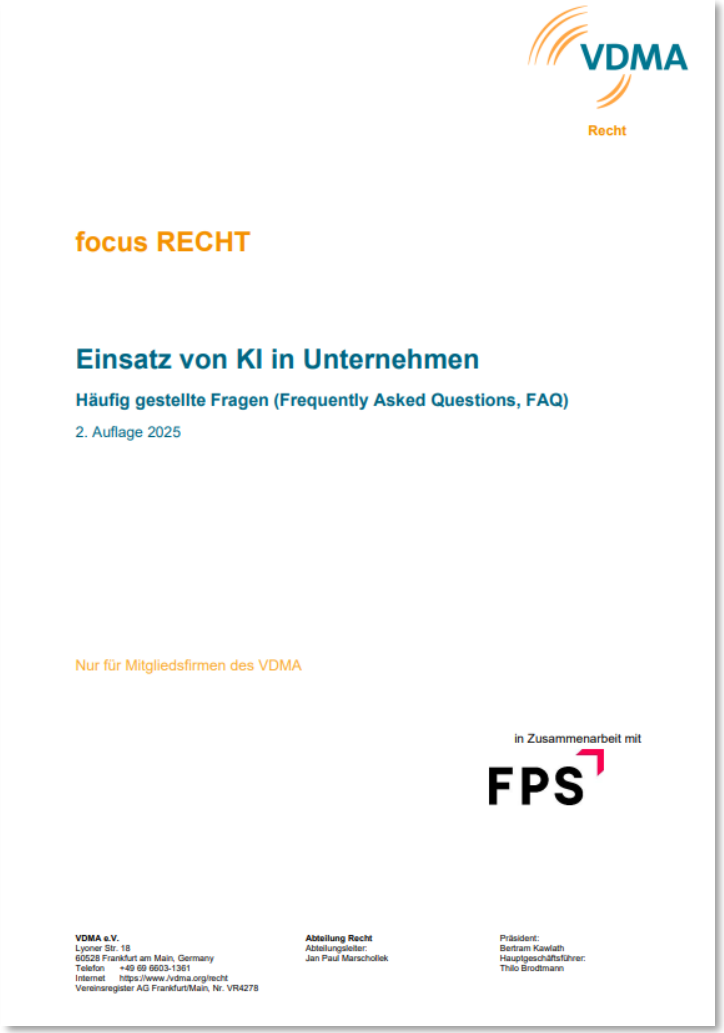
- **VDMA-FAQ zur KI-Verordnung:**

  https://www.vdma.org/viewer/-/v2article/render/91653664
- **VDMA AK digitaLegis:**

  https://vdma.org/groups-details/-/group/73551
- **VDMA Newsletter „Legal“:**

→ *Abonnieren unter „MyVDMA / Newsletter“ https://vdma.org/personal-space*

- **Checkliste für Betreiber** (kommt bald)


VDMA
Recht

focus RECHT

Einsatz von KI in Unternehmen

Häufig gestellte Fragen (Frequently Asked Questions, FAQ)

2. Auflage 2025

Nur für Mitgliedsfirmen des VDMA

in Zusammenarbeit mit
FPS

VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main, Germany
Telefon +49 69 6603-1361
Internet https://www.vdma.org/recht
Vereinsregister AG Frankfurt/Main, Nr. VR4278

Abteilung Recht
Abteilungsleiter:
Jan Paul Marscholleck

Präsident:
Bertram Kawlath
Hauptgeschäftsführer:
Thilo Brodtmann

KONTAKT

Danke für Ihre Aufmerksamkeit.

FÜR WEITERE INFORMATION MELDEN SIE SICH GERNE BEI:

Dr. Jacob L. Gorenflos López
Policy Officer for Technical Regulation

VDMA e.V.
Division for Technical Regulation and Standardisation

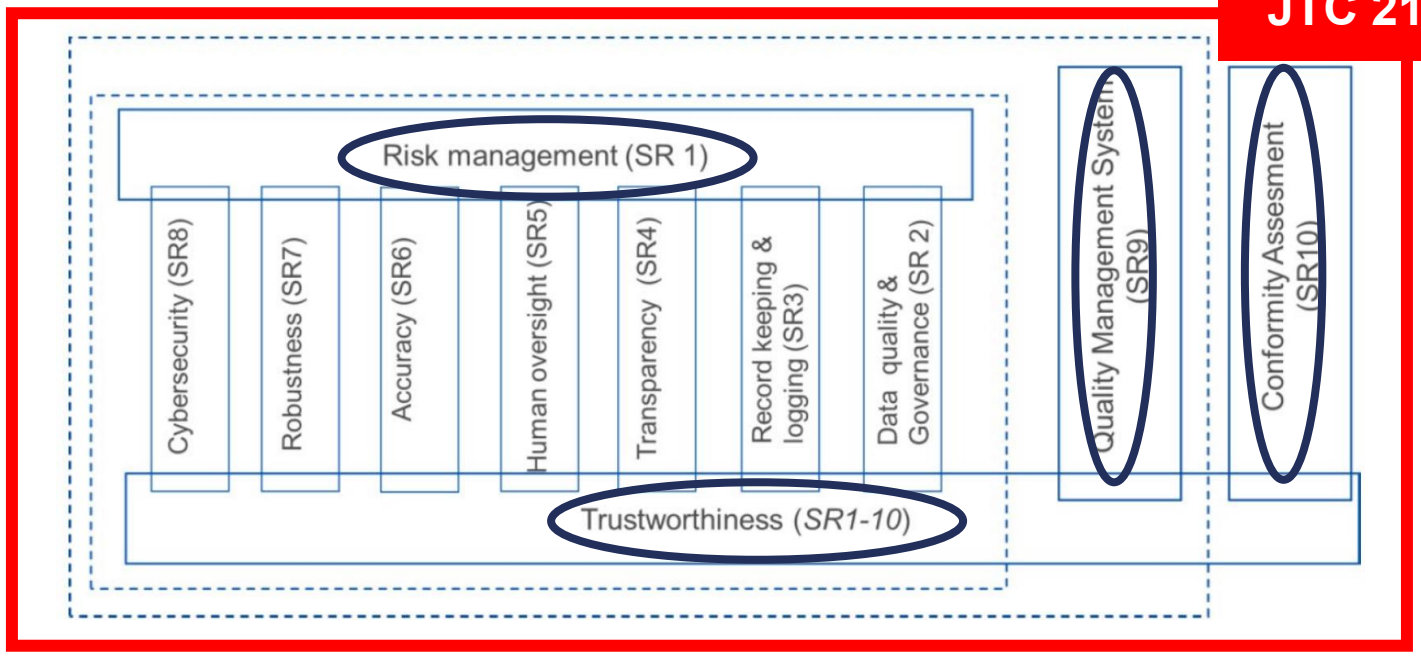
Friedrichstraße 95
10117 Berlin
Germany

+49 0170 5216147
Jacob.gorenflos-lopez@vdma.eu
vdma.eu

Inhalt des Standardisation Request (SReq)

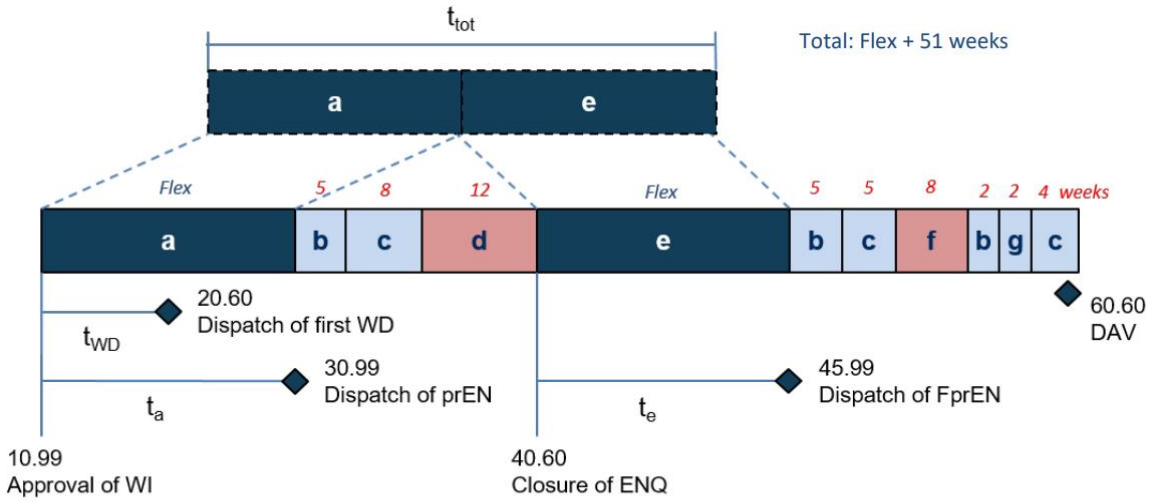
1. **risk management** system for AI systems
2. **governance and quality** of datasets used to build AI systems
3. **record keeping** - built-in logging capabilities in AI systems
4. **transparency and information** to the users of AI systems
5. **human oversight** of AI systems
6. **accuracy** specifications for AI systems
7. **robustness** specifications for AI systems
8. **cybersecurity** specifications for AI systems
9. **quality management** system for providers of AI system
10. **conformity assessment** for AI systems

JTC 21 Folie



further items:
– sustainability of AI
– generative AI

WD bis Publikation



a	Drafting of prEN		Internal process
b	Editing		Technical work
c	Translation and preparation of national publication		Voting
d	Enquiry		
e	Comments handling / preparation of FprEN		
f	Formal Vote		
g	TC proofing		

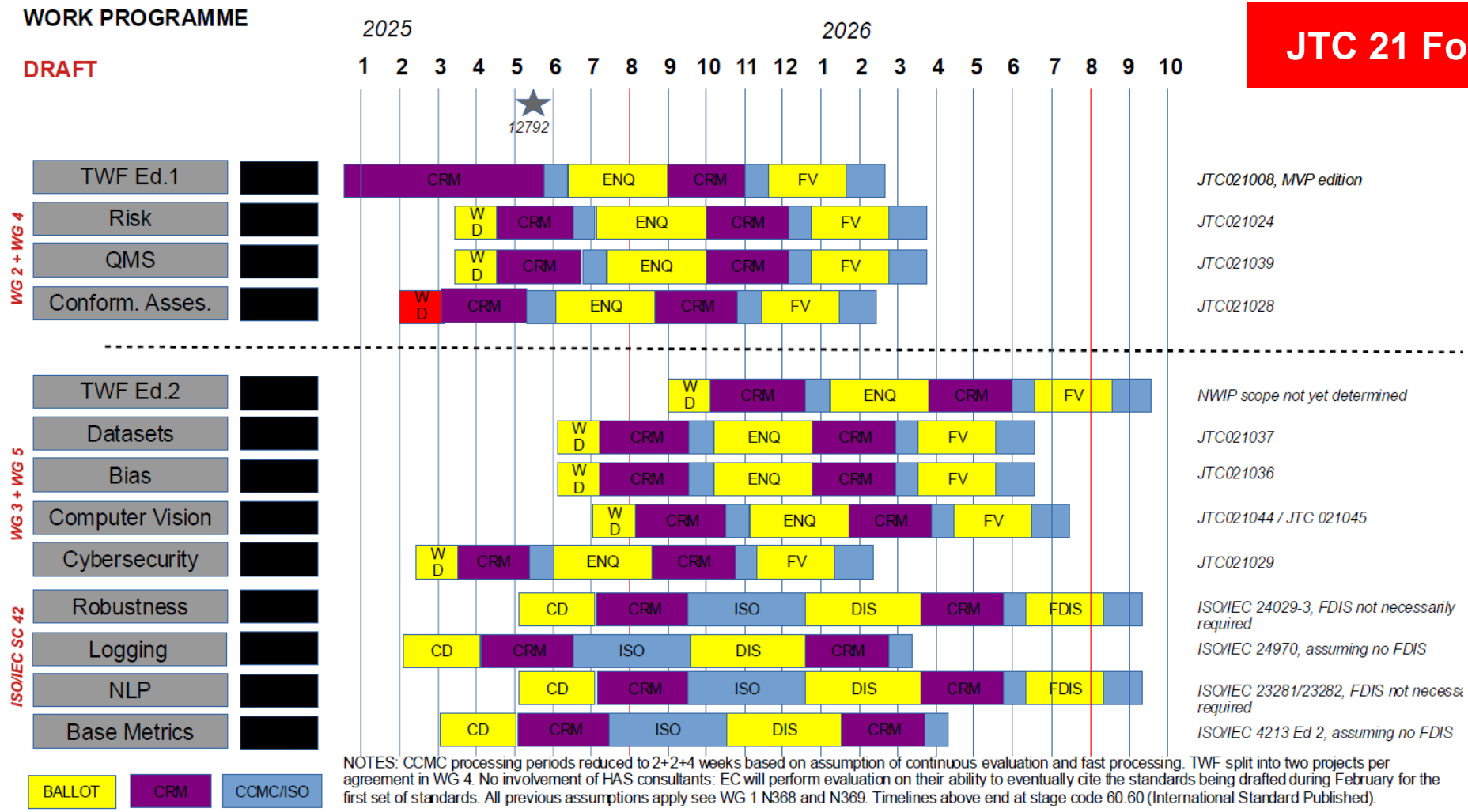
Konzessionen an KI-Normung

1. Übersetzung wird nachträglich angefertigt
2. Administratives Fasttracking in CCMC
3. Kein HAS-Assessment

Prozessschritt	„Normaler Prozess“	JTC 21 Annahme
Dispatch of first WD	4 Wochen	4 Wochen
1. Comment Resolution Meeting (CRM)	Schwer vorhersehbar (bis 34 Wochen)	10 Wochen für TWF wurden 5 Monate angesetzt
1. Administrative Phase	13 Wochen	**2 Wochen**
Enquiry	12 Wochen	12 Wochen
2. CRM	Schwer vorhersehbar (bis 34 Wochen)	10 Wochen
2. Administrative Phase	10 Wochen	**2 Wochen**
Formal Vote	8 Wochen	8 Wochen
3. Administrative Phase	11 Wochen	**4 Wochen**
Σ =	**78 Wochen (CRM Annahmen wie JTC 21) bis 128 Wochen**	**52 Wochen**

Vorgeschlagenes Arbeitsprogramm vom 4. Februar 2025

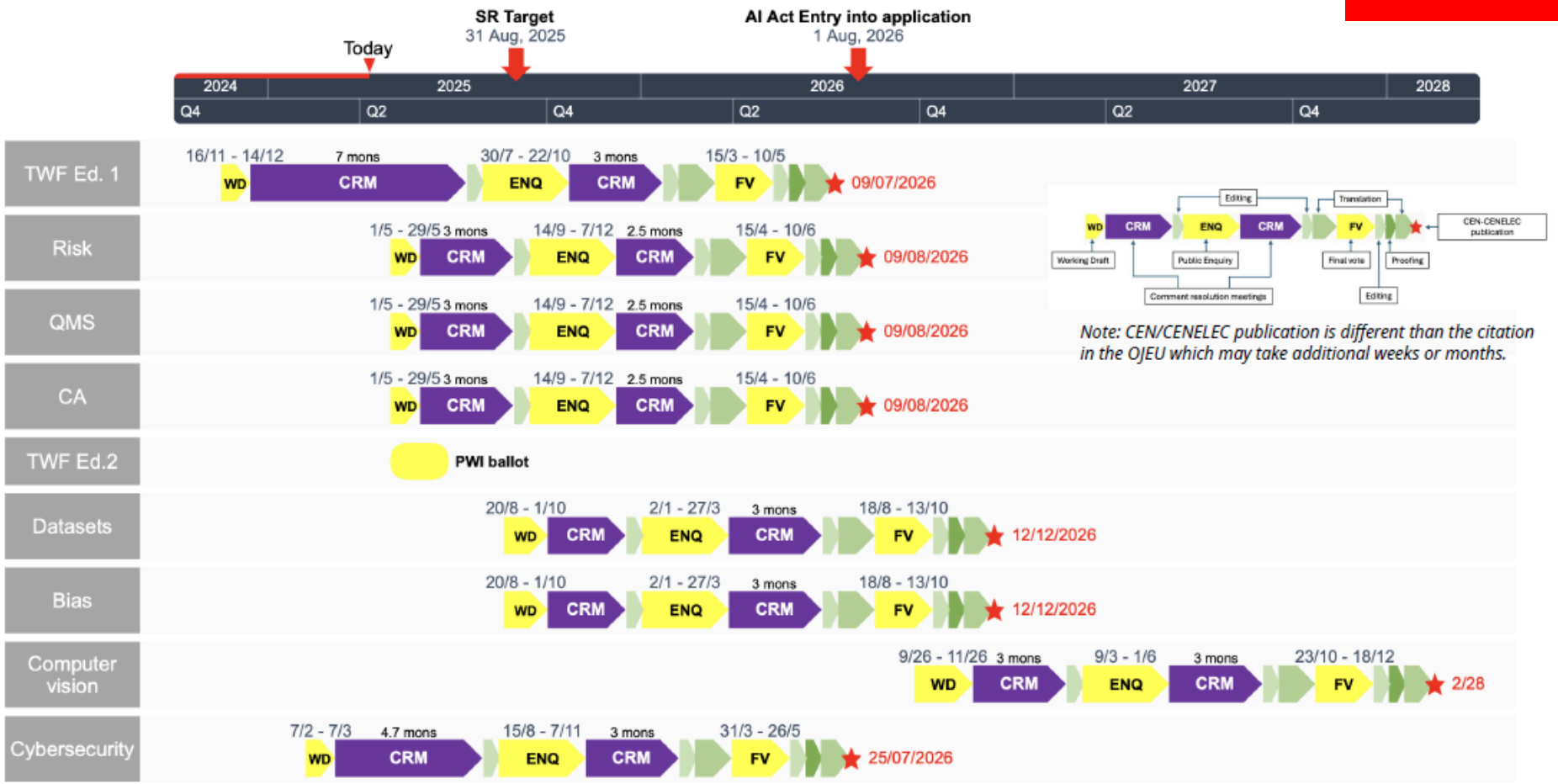
JTC 21 Folie



NOTES: CCMC processing periods reduced to 2+2+4 weeks based on assumption of continuous evaluation and fast processing. TWF split into two projects per agreement in WG 4. No involvement of HAS consultants: EC will perform evaluation on their ability to eventually cite the standards being drafted during February for the first set of standards. All previous assumptions apply see WG 1 N368 and N369. Timelines above end at stage code 60.60 (International Standard Published).

Arbeitsprogramm vom 13. April 2025

JTC 21 Folie

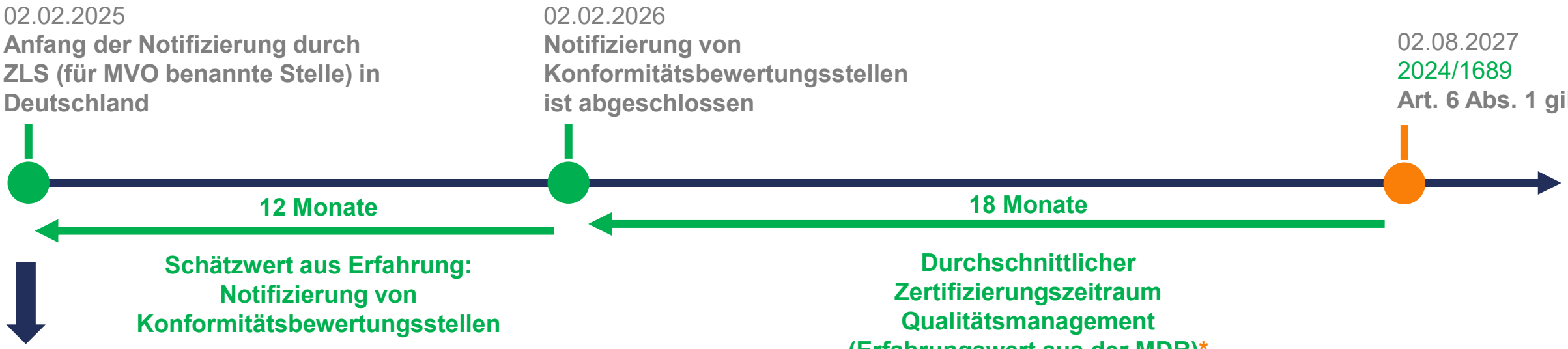


Vergleich der Arbeitsprogramme von home-grown hEN

Metrik: Projizierter Abschluss

	04. Februar	13. April	Δ
TWF Ed. 1	22.02.2026	09.07.2026	**4.5 Monate**
Risk	22.03.2026	09.08.2026	**4.5 Monate**
QMS	22.03.2026	09.08.2026	**4.5 Monate**
CA	15.02.2026	09.08.2026	**4.75 Monate**
Datasets	15.06.2026	12.12.2026	**6 Monate**
Bias	15.06.2026	12.12.2026	**6 Monate**
Computer Vision	15.07.2026	01.02.2028	**16.5 Monate**
Cybersecurity	15.02.2026	25.07.2026	**5.5 Monate**

Wann sollten die hEN fertig sein?



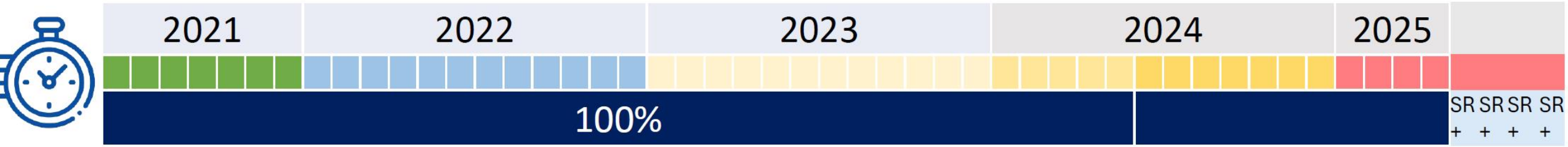
Bauen ihr Notifizierungskonzept gerne auf hEN auf.

2024/1689 KI-Verordnung

*Zahlen und Fakten zur MDR - BVMed

Folien der EU Kommission

Plan A – Harmonised Standards Timeline and Deliverables



AI Act application

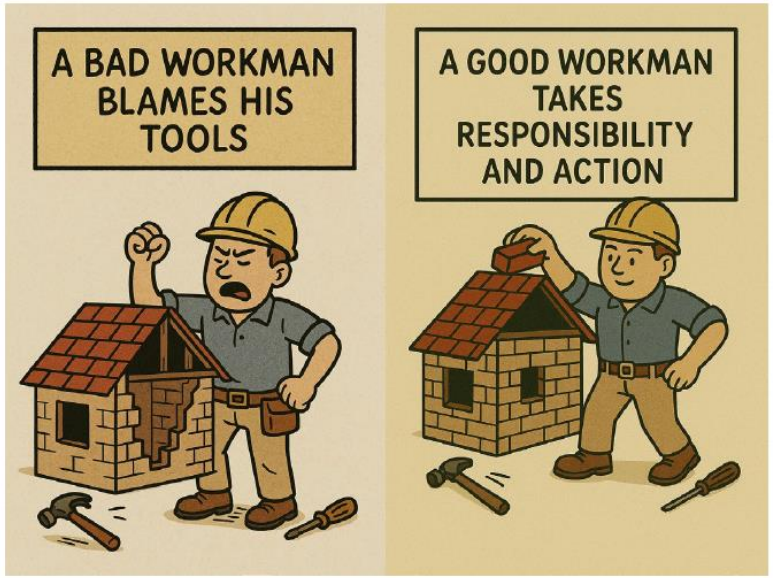
August 2026 ***Annex III***

August 2027 ***Annex I***

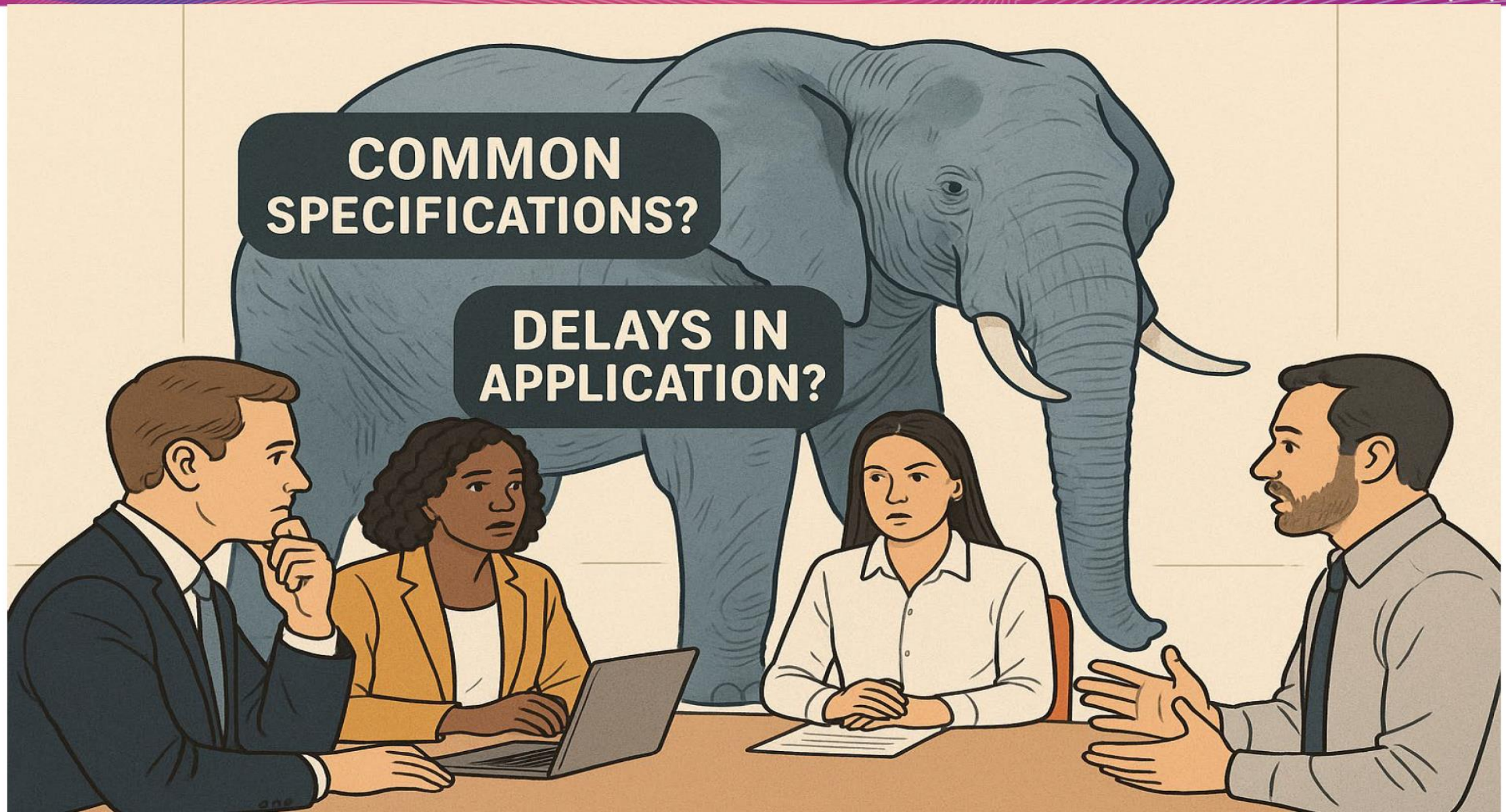
AI is a complex topic
Yes – but

34

Published ISO standards *



What is a plan B?



Folien der EU Kommission

Plan B

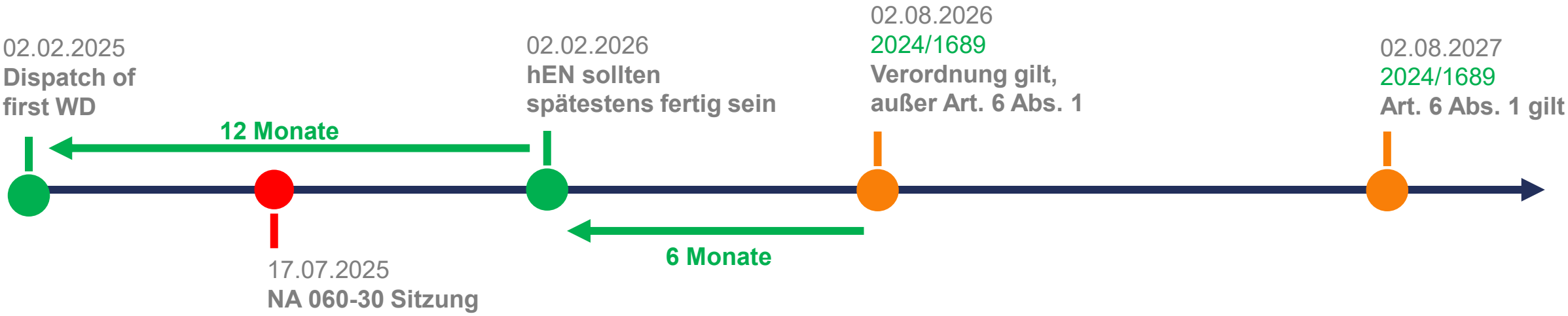
Plan A = B → Harmonised Standards

Accelerate the work on all 10 standardisation areas

–

strong concerns of the EC, Member States and other stakeholders with the slow progress in the JTC-21

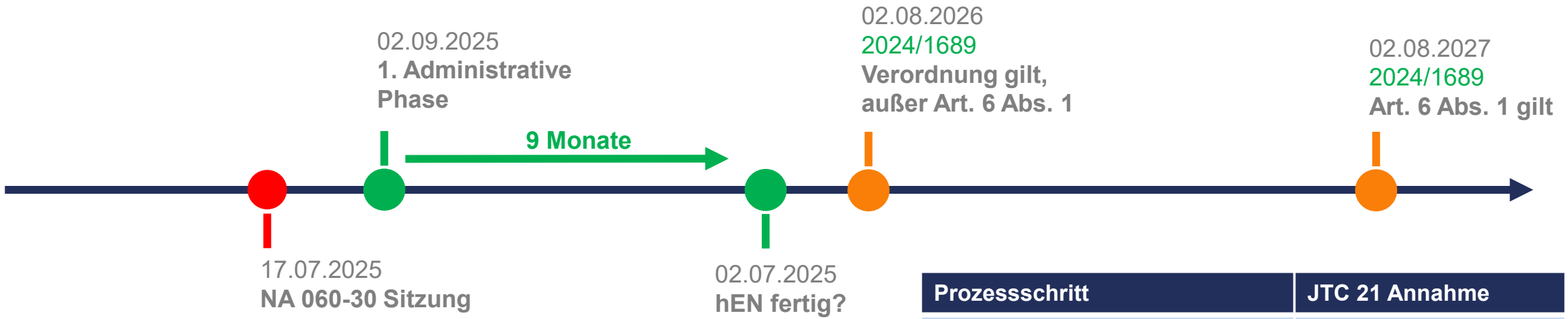
Wann sollten die hEN fertig sein?



Prozessschritt	„Normaler Prozess“	JTC 21 Annahme
Σ =	78 Wochen (CRM Annahmen wie JTC 21) bis 128 Wochen	52 Wochen

2024/1689 KI-Verordnung

Wann sollten die hEN fertig sein?



Prozessschritt	JTC 21 Annahme
1. Administrative Phase	2 Wochen
Enquiry	12 Wochen
2. CRM	10 Wochen
2. Administrative Phase	2 Wochen
Formal Vote	8 Wochen
3. Administrative Phase	4 Wochen
Σ =	38 Wochen

Im September sollen die ersten zwei prEN in die 1. Administrative Phase kommen

2024/1689 KI-Verordnung