Die EU-Maschinenverordnung -

Neue Entwicklungen und Schnittstellen in der Product Compliance

20. Mai 2026

Dipl.-Ing. (FH) Martin Launer
Jann Karrasch

The Legal Engine

Powered by Osborne Clarke

Zukunftsallianz Maschinenbau
FIT FOR FUTURE MARKETS

Inhalt

Vorstellungsrunde

I. Vorstellungsrunde

Dipl.-Ing. (FH) Martin Launer
Rechtsanwalt / Partner
Hamburg

+49 40 55436 4126
martin.launer@osborneclarke.com

- Studium der Schiffsbetriebstechnik in Flensburg und Seefahrtszeit als Ingenieur auf Containerschiffen;
- Studium der Rechtswissenschaft in Kiel und parallele Tätigkeit als Ingenieur an der FH in Kiel (Institut für Werkstoffkunde) und am „GEOMAR“ Helmholtz-Zentrum für Meereswissenschaften;
- Zulassung und Tätigkeit als Rechtsanwalt seit 2000.

Jann Karrasch
Rechtsanwalt / Associate
Hamburg

+49 40 55436 4228
jann.karrasch@osborneclarke.com

- Studium der Rechtswissenschaft in Hamburg im Schwerpunktbereich Handels- und Gesellschaftsrecht;
- Referendariat am Oberlandesgericht Celle mit Stationen u.a. in US-amerikanischer Großkanzlei in Chicago;
- Zulassung und Tätigkeit als Rechtsanwalt seit 2024 im Hamburger Büro von Osborne Clarke in der Praxisgruppe Commercial.

I. Vorstellungsrunde

Dipl.-Ing. (FH) Martin Launer
Rechtsanwalt / Partner
Hamburg

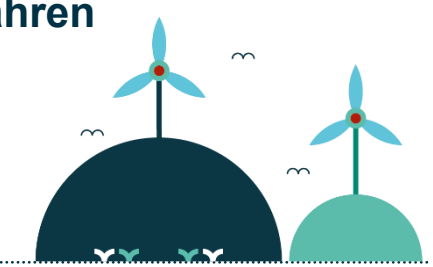
+49 40 55436 4126
martin.launer@osborneclarke.com

Jann Karrasch
Rechtsanwalt / Associate
Hamburg

+49 40 55436 4228
jann.karrasch@osborneclarke.com

Beratungsschwerpunkte

- **Beratung des Maschinen- und Anlagenbaus**, sowohl landseitig als auch im maritimen Sektor
- Gerichtliche und außergerichtliche Abwicklung von Schadensfällen (Hersteller, Zulieferer und Versicherer)
- **Beratung des Maschinen- und Anlagenbaus** in **Fragen der Produkthaftung, Produktsicherheit, CE-Compliance** und **Übergang zur MVO**
- **Claim Management** für Maschinen- und Anlagenbauer, inklusive internationaler **Schiedsverfahren**
- Rechtliche Begleitung von **Produkthaftungsfällen**, auch in den USA
- Inhouse-Seminare und Vertragsvorlagen, u.a. für den **VDMA**



(Kurzer) Einblick in unsere anwaltliche Praxis

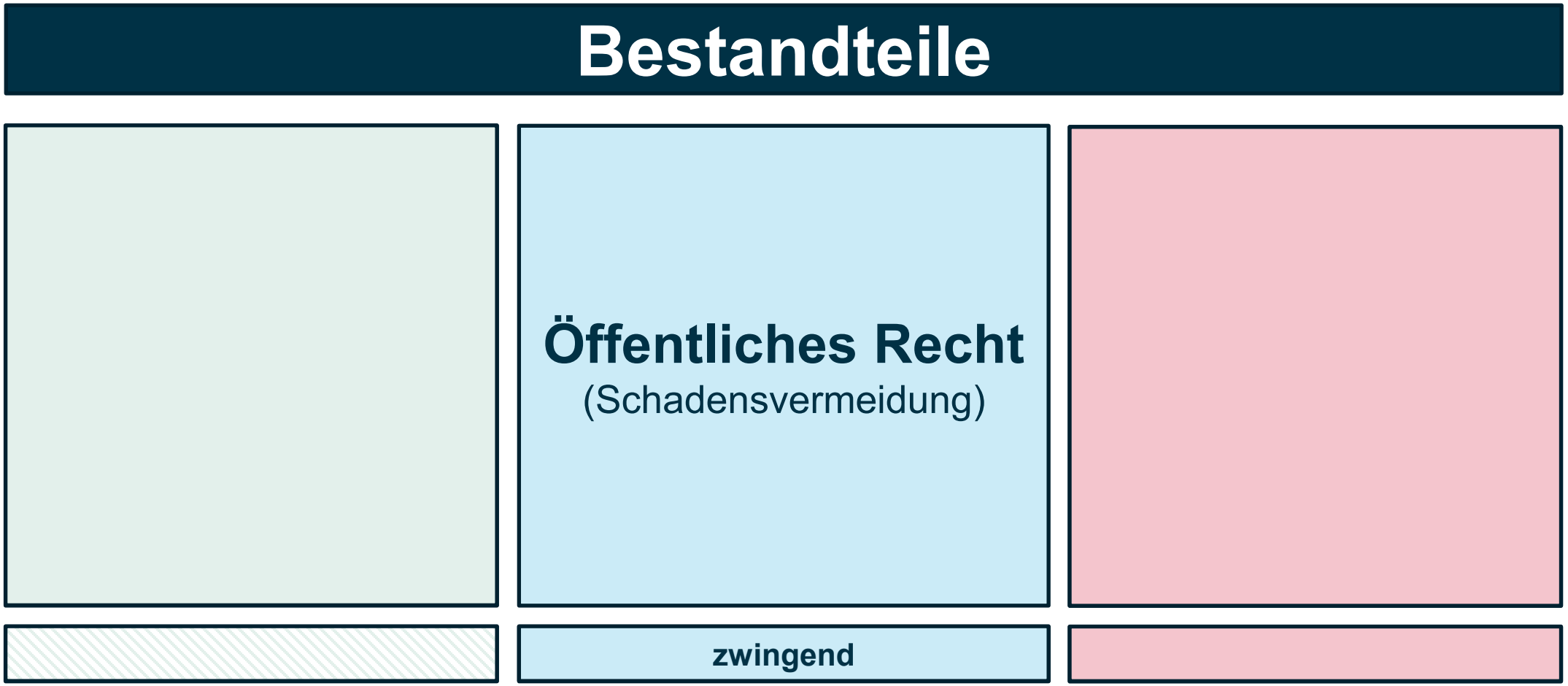
(Kurzer) Einblick in unsere anwaltliche Praxis

(Kurzer) Einblick in unsere anwaltliche Praxis

Basics der Produkthaftung

II. Basics der Produkthaftung

1. Rechtsgebiete



II. Basics der Produkthaftung

1. Rechtsgebiete

II. Basics der Produkthaftung

2. Relevante Rechtsbeziehungen

II. Basics der Produkthaftung

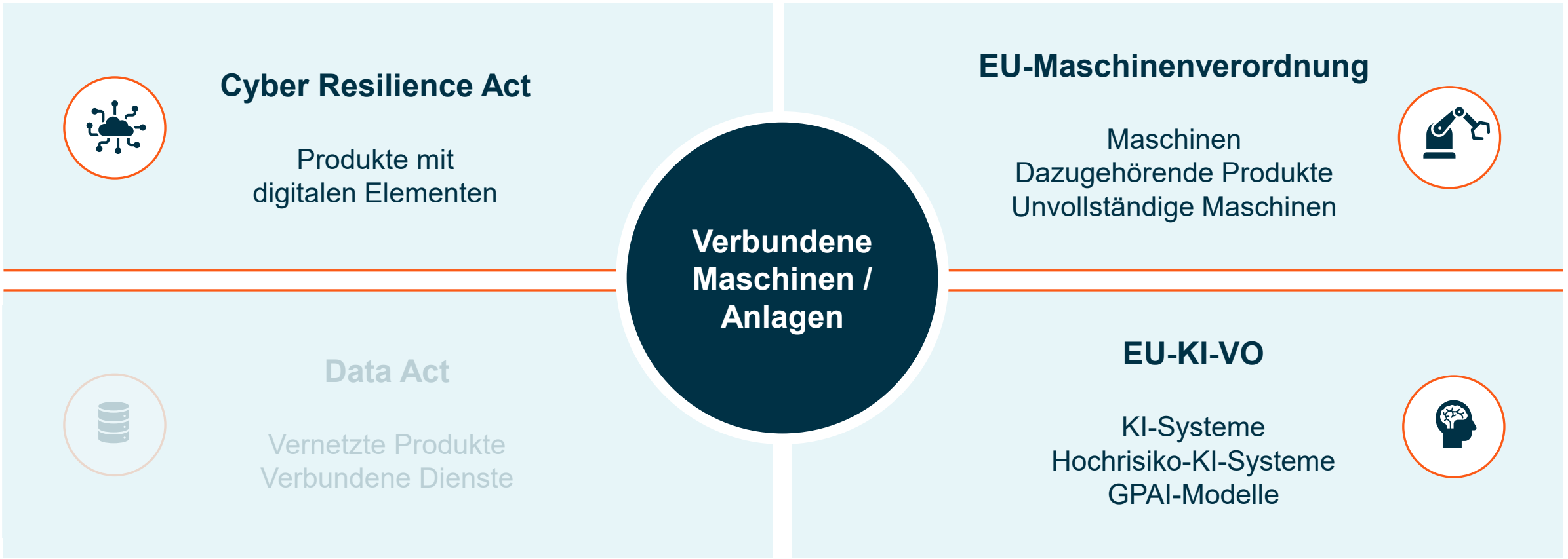
3. Rechtsgrundlagen

- **Gesetze / Richtlinien / Verordnung** sind **für Jedermann verpflichtend**; direkt einschlägig
- (Technische) **Normen / Standards** sind **grds. freiwillig** (im Gegensatz zu den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen des EU-Rechts!)
  - Gleichzeitig Konformitätsvermutung bei harmonisierten Normen sehr relevant
  - Gerichte verwenden Normen / Standards oftmals als **Maßstab für Fahrlässigkeit**!
  - Gelten grenzüberschreitend / weltweit, da sie i.d.R. nicht von Staaten, sondern von privaten Organisationen herausgegeben werden

Cybersecurity und KI in Maschinen und Anlagen

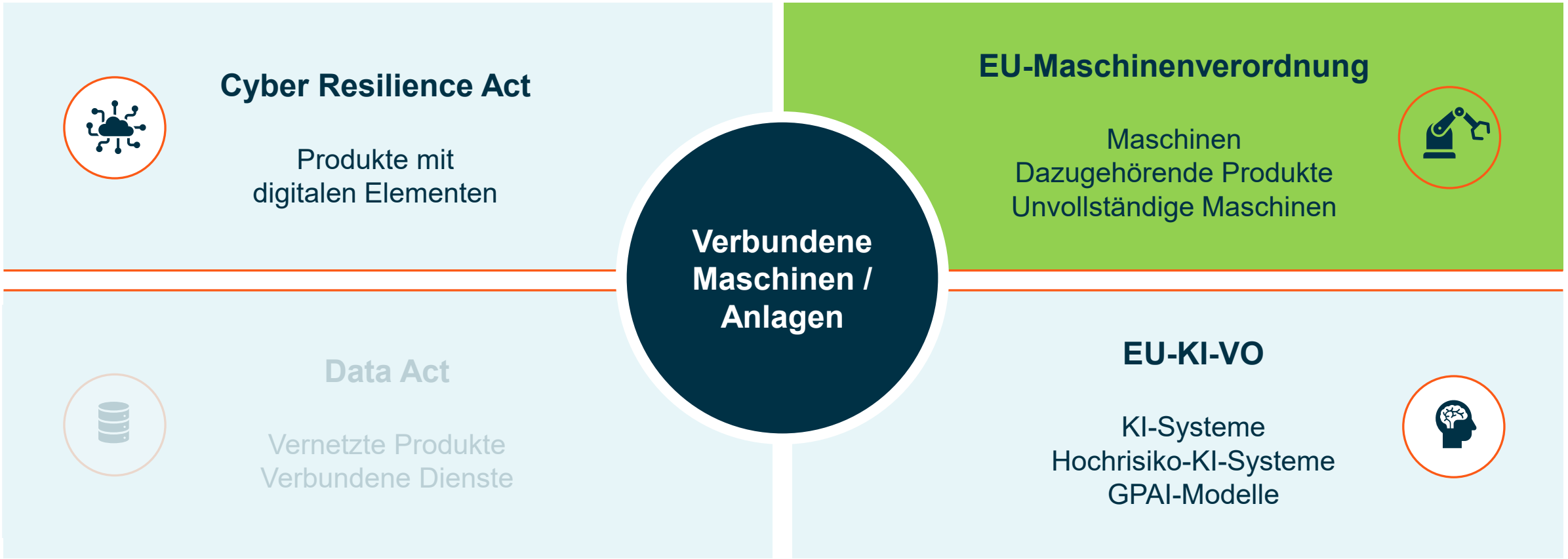
III. Cybersecurity und KI in Maschinen und Anlagen

1. EU-Recht: Überschneidung der Anwendungsbereiche



III. Cybersecurity und KI in Maschinen und Anlagen

1. EU-Recht: Überschneidung der Anwendungsbereiche



Maschinenverordnung – In a nutshell

Die **MVO** regelt das **Inverkehrbringen von Maschinen und verwandten Produkten in der Europäischen Union**. Ziel ist es, ein hohes Sicherheitsniveau zu gewährleisten, den freien Warenverkehr zu fördern und die Vorschriften an den technologischen Fortschritt anzupassen.

III. Cybersecurity und KI in Maschinen und Anlagen

2. Die EU-Maschinenverordnung („**MVO**“)

- Verordnung = europaweit **unmittelbare Geltung** ab 20. Januar 2027
- **Keine Übergangsfrist**, zwingend anwendbar bei Inverkehrbringen
  - Keine vertragliche Abweichung möglich
  - Möglicherweise „Stichtagsprobleme“ bei Legacy-Modellen
  - Anwendbarkeit auch möglich nach wesentlichen Veränderungen ab Inkrafttreten
  - Berücksichtigung in der Konstruktionsphase bereits so früh wie möglich
- Deutlich erhöhte Regelungsdichte (Anzahl der **Artikel in etwa verdoppelt**)
  - Differenzierung in „Maschinen“ und „**dazugehörige Produkte**“
  - Vorgaben zur **Cybersecurity** + **KI-Integration** in Maschinen
  - **Digitale** Betriebsanleitung + EU-Konformitätserklärung vorgesehen
  - Explizite Regelung der „**wesentlichen Veränderung**“

III. Cybersecurity und KI in Maschinen und Anlagen

2. Die EU-Maschinenverordnung („**MVO**“)

Anforderungen an Cybersecurity

- Weiter Anwendungsbereich: „Sicherheitsbauteil“ = **physisch** oder **digital**, einschließlich **Software**
- Eingriffe Dritter
  - Angemessener Schutz gegen „unbeabsichtigte oder vorsätzliche **Korrumpierung**“
  - Bezogen auf Software und Daten sowie Hardwarebauteile, die Signale/Daten übertragen
  - **Sammeln von Nachweisen** für rechtmäßiges oder unrechtmäßiges Eingreifen
  - Auch für unvollständige Maschinen, wenn Vorgaben schon vor Einbau erfüllbar

III. Cybersecurity und KI in Maschinen und Anlagen

2. Die EU-Maschinenverordnung („**MVO**“)

Anforderungen an Cybersecurity

- Resilienz von Steuerungen
  - Müssen **Fremdeinflüssen standhalten** können
  - Einschließlich vernünftigerweise vorhersehbare **Versuche Dritter**, die zu einer **Gefährdungssituation** führen können
  - Steuerungen müssen **Rückverfolgungsprotokoll** erstellen (mind. 5 Jahre bereithalten)

III. Cybersecurity und KI in Maschinen und Anlagen

2. Die EU-Maschinenverordnung („**MVO**“)

KI-gestützte Komponenten

- Was versteht die MVO unter „KI“?
  - Vollständig oder teilweise **selbstentwickelndes Verhalten + maschinelles Lernen**
  - **Nicht**, wenn System weder lern- noch entwicklungsfähig ist
  - **Nicht**, wenn nur zur Ausführung bestimmter automatisierter Funktionen programmiert
  - **Nicht**, wenn System bereits „austrainiert“ ist, sich nicht mehr weiterentwickelt
  - **Nicht**, wenn andere Verfahren von KI zum Einsatz kommen

III. Cybersecurity und KI in Maschinen und Anlagen

2. Die EU-Maschinenverordnung („**MVO**“)

KI-gestützte Komponenten

- Praktische Konsequenzen bei KI-Einsatz (Anhang I, Teil A MVO)

  - Bei Verwendung von KI in…
    - …***Sicherheitsbauteilen*** *(einschließlich Software), und/oder*
    - *…ab Auslieferung* ***eingebetteten Sicherheitssystemen***

    zwingend Konformitätsbewertungsverfahren mit **notifizierten Stellen** (Art. 25 Abs. 2 MVO)

III. Cybersecurity und KI in Maschinen und Anlagen

2. Die EU-Maschinenverordnung („**MVO**“)

KI-gestützte Komponenten

- Praktische Konsequenzen bei KI-Einsatz (Anhang I, Teil A MVO)

  - Selbstentwickelnd + teilweise autonom: System kann sich permanent verändern
    - *„Die Risikobeurteilung und Risikominderung umfassen Gefährdungen, die **im Laufe des Lebenszyklus der Maschinen auftreten können** und die zum Zeitpunkt ihres Inverkehrbringens vorhersehbar sind, da sie sich aus (…) selbstentwickelndem Verhalten oder (…) selbstentwickelnder Logik (…) ergeben.“* (Anhang III, Teil B Ziff. 1 MVO)
  - Hersteller muss bereits in der Konstruktionsphase geplante **Aktualisierungen** oder (Software-)**Weiterentwicklungen** berücksichtigen

III. Cybersecurity und KI in Maschinen und Anlagen

2. Die EU-Maschinenverordnung („**MVO**“)

KI-gestützte Komponenten

- Anforderungen an selbstentwickelnde oder autonome **Steuerungssysteme**
  - Keine Handlungen über festgelegten Bewegungsbereich hinaus
  - Keine Verschiebung der Grenzen von Sicherheitsfunktionen
  - Aufzeichnungen von Daten von sicherheitsrelevanten Entscheidungsprozessen
- Anforderungen an die **Ergonomie**
  - Reaktionen auf Worte / Gesten / Gesichtsausdrücke / Körperbewertungen des Bedieners
  - Geplante Handlungen verständlich mitteilen (*was System tut und warum*)
- Vorgaben für **autonome mobile Maschinen**
  - Vorhandensein permanenter Überwachungsfunktion, z.B. Remote-Steuerung
  - Relevante Sicherheitsfunktionen müssen auch ohne Interaktion des Bedieners erfolgen können

III. Cybersecurity und KI in Maschinen und Anlagen

Cyber Resilience Act

Produkte mit
digitalen Elementen

EU-Maschinenverordnung

Maschinen
Dazugehörende Produkte
Unvollständige Maschinen

Verbundene Maschinen / Anlagen

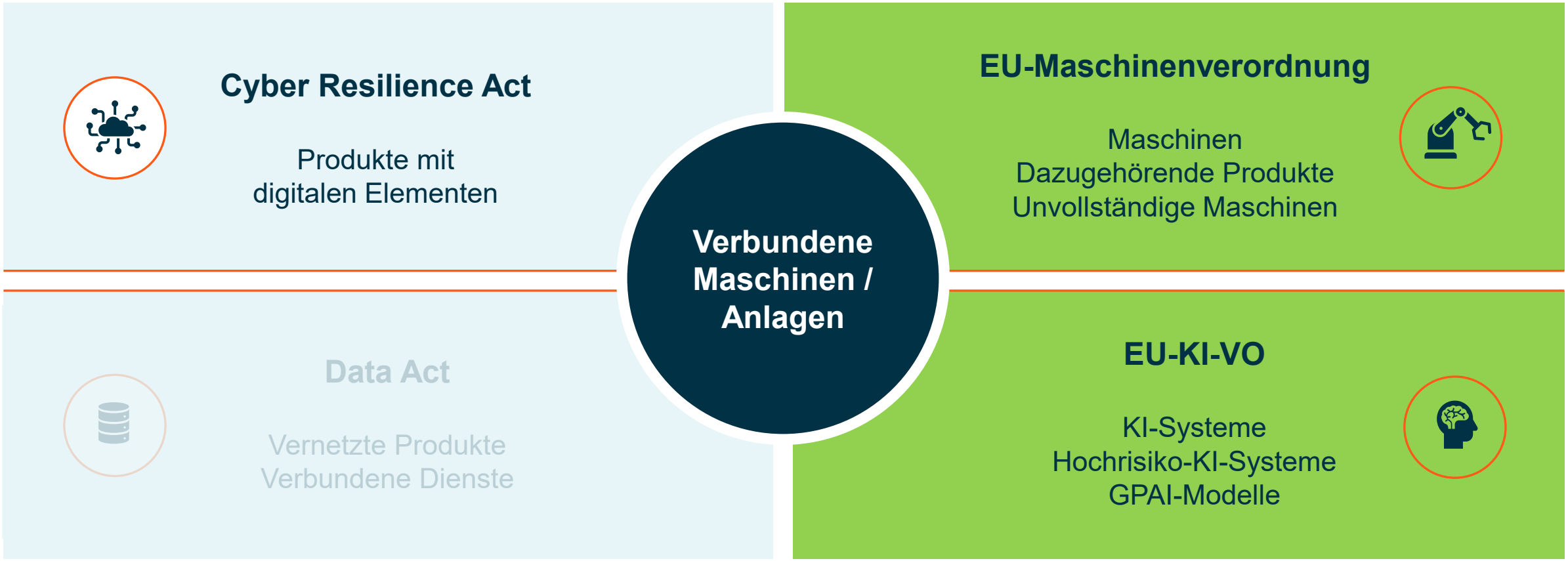
Data Act

Vernetzte Produkte
Verbundene Dienste

EU-KI-VO

KI-Systeme
Hochrisiko-KI-Systeme
GPAI-Modelle

III. Cybersecurity und KI in Maschinen und Anlagen



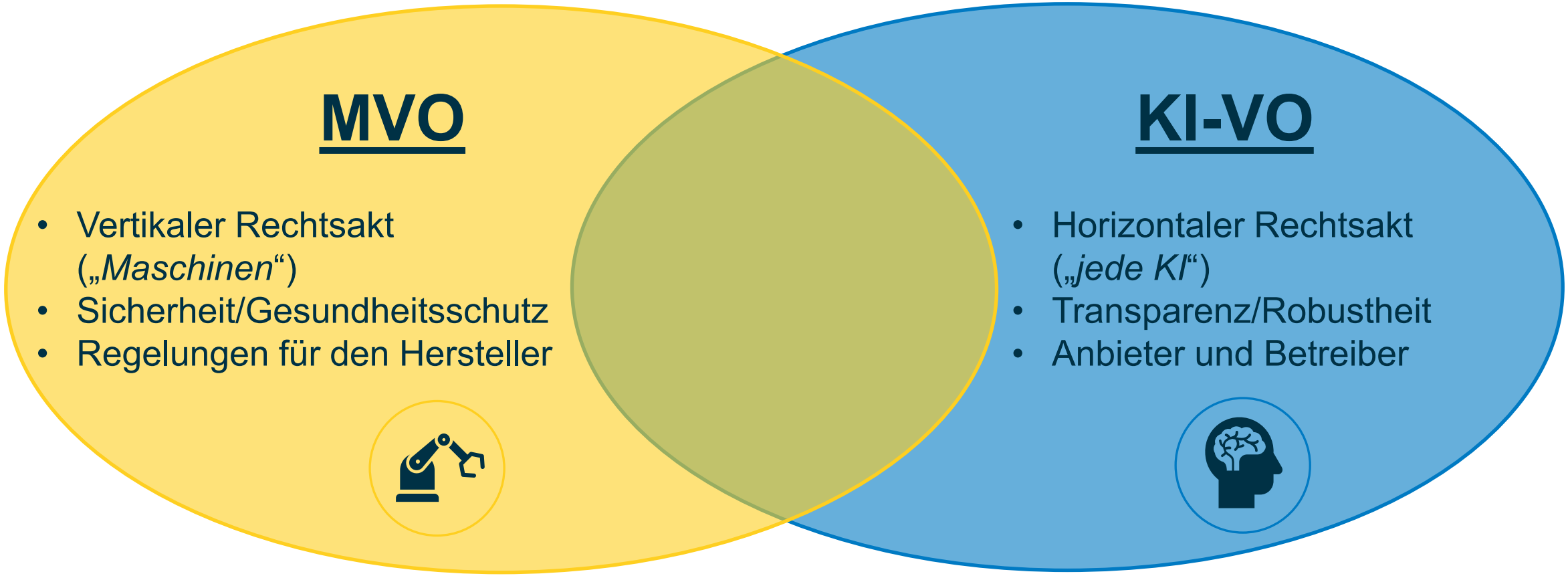
EU-KI-VO – In a nutshell

Die **EU-KI-VO** regelt die **Entwicklung, Bereitstellung und Nutzung von Künstlicher Intelligenz** in der Europäischen Union. Ziel ist es, Innovation zu fördern, Vertrauen in KI-Systeme zu stärken und zugleich die Sicherheit, Grundrechte und Rechtsstaatlichkeit zu gewährleisten.

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Überschneidung der Anwendungsbereiche



III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Überschneidung der Anwendungsbereiche

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Grundlagen

- KI-VO als sog. **horizontaler Rechtsakt** der EU
  - Reglementiert sämtliche KI-Systeme, die für einen autonomen Betrieb ausgelegt sind
  - Unabhängig davon, ob sie anpassungsfähig sind / technologieoffen
- Hersteller-Begriff („**Anbieter**“) vergleichbar zum bekannten Maschinenrecht
  - Wer bei Dritten beauftragt, aber unter eigenem Namen in Verkehr bringt, zählt als Hersteller
- Differenzierung in Risiko-Klassen
  - „**Hochrisiko-KI-Systeme**“ gem. Anhang I, Teil A zur KI-VO
  - „Eigenständige KI-Systeme“
  - „KI-Modelle mit allgemeinem Verwendungszweck“
  - Alle sonstigen Arten von KI-Systemen

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Zeitlicher Anwendungsbereich

- Mehrheit der Vorschriften zu Hochrisiko-KI-Systemen ursprünglich: **2. August 2027**
- Problem: EU-Kommission hat **bislang keine Leitlinien** zur KI-VO herausgegeben, harmonisierte Normen und gemeinsame Spezifikationen befinden sich noch in der Abstimmung
  - ➢ „**Digital Omnibus on AI**“: Pflichten für Maschinen greifen erst **zwölf Monate** nach Verfügbarkeit unterstützender Maßnahmen der EU-Kommission – **spätestens ab 2. August 2028** *(Entwurfsstand November 2025)*

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Relevanz von Hochrisiko-KI-Systemen

- Soweit keine verbotenen Praktiken zum Einsatz kommen: „Nur“ **Kompetenzanforderungen** und **Transparenzpflichten**
- Demgegenüber **umfangreiche technische Regelungen** und Maßgaben für **Hochrisiko-KI**
  - **Anhang I**, Abschnitt A KI-VO listet Maschinenrichtlinie (damit auch die MVO)
  - Art. 6 Abs. 1 KI: **KI-System gilt immer als Hochrisiko-KI-System**, wenn…
    - *„es als **Sicherheitsbauteil** eines unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet werden soll“*;

      +

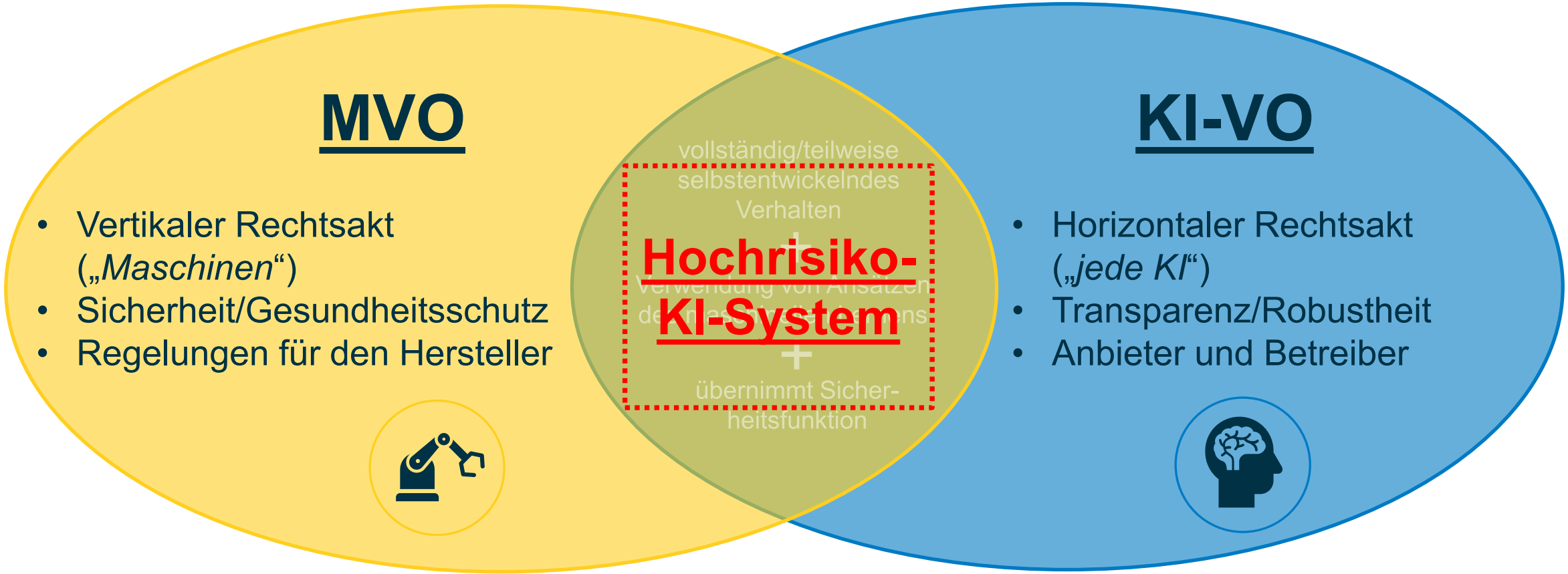
    - *„das Gesamtprodukt oder das KI-System selbst als Produkt muss einer **Konformitätsbewertung durch Dritte** unterzogen werden“*

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)



III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Relevanz von Hochrisiko-KI-Systemen

- Art. 25 Abs. 3 KI-VO: Enthält Maschine ein Hochrisiko-KI-System als Sicherheitsbauteil und wird **unter dem Namen des Herstellers** zusammen mit der Maschine in Verkehr gebracht oder in Betrieb genommen
  - ➢ Maschinenhersteller **gilt auch als Hersteller** („Anbieter“) **des Hochrisiko-KI-Systems!**

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Compliance-Pflichten der Hersteller (Hochrisiko-KI-Systeme)

- **Risikomanagementsystem**, das gesamten Lebenszyklus umfasst
- System und Plan zur **Beobachtung nach Inverkehrbringen**
- Besondere Transparenz- und **Aufzeichnungspflichten** („Protokollierung“)
  - Aufzeichnung von Ereignissen, für Erleichterung von Produktbeobachtung und Betriebsüberwachung
- Systeme müssen von natürlichen Personen **wirksam beaufsichtigt werden können** (HMI)
- **Genauigkeit, Robustheit und Cybersicherheit** während des **gesamten Lebenszyklus**

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Verzahnungen zwischen MVO und KI-VO (Hochrisiko-KI-Systeme)

- Art. 8 Abs. 2 S. 2 KI-VO:

> *„Im Hinblick auf (…) **Vermeidung von Doppelarbeit** und der **Minimierung zusätzlicher Belastungen** haben die Anbieter die Wahl, die erforderlichen (…) Informationen und Dokumentationen (…) gegebenenfalls **in Dokumentationen** (…) **zu integrieren, die bereits bestehen** und (…) in [anderen] Harmonisierungsrechtsvorschriften der Union vorgeschrieben sind.“*

III. Cybersecurity und KI in Maschinen und Anlagen

3. Die EU-KI-Verordnung („**KI-VO**“)

Verzahnungen zwischen MVO und KI-VO (Hochrisiko-KI-Systeme)

- Nur eine einzige technische Dokumentation (nach allen Vorschriften) **für die gesamte Maschine**
- Auch für KI-VO gelten die **Ausnahmen von Konformitätsbewertungsverfahren** aus der MVO
- Produktbeobachtung: Rückgriff auf **System/Plan nach MVO** (falls vorhanden und gleichwertig)
- **Marktüberwachungsbehörde** nach MVO auch für Hochrisiko-KI-System zuständig
- EU-Kommission wird „Leitlinie für die praktische Umsetzung“ veröffentlichen

III. Cybersecurity und KI in Maschinen und Anlagen

Cyber Resilience Act

Produkte mit
digitalen Elementen

EU-Maschinenverordnung

Maschinen
Dazugehörende Produkte
Unvollständige Maschinen

Verbundene Maschinen / Anlagen

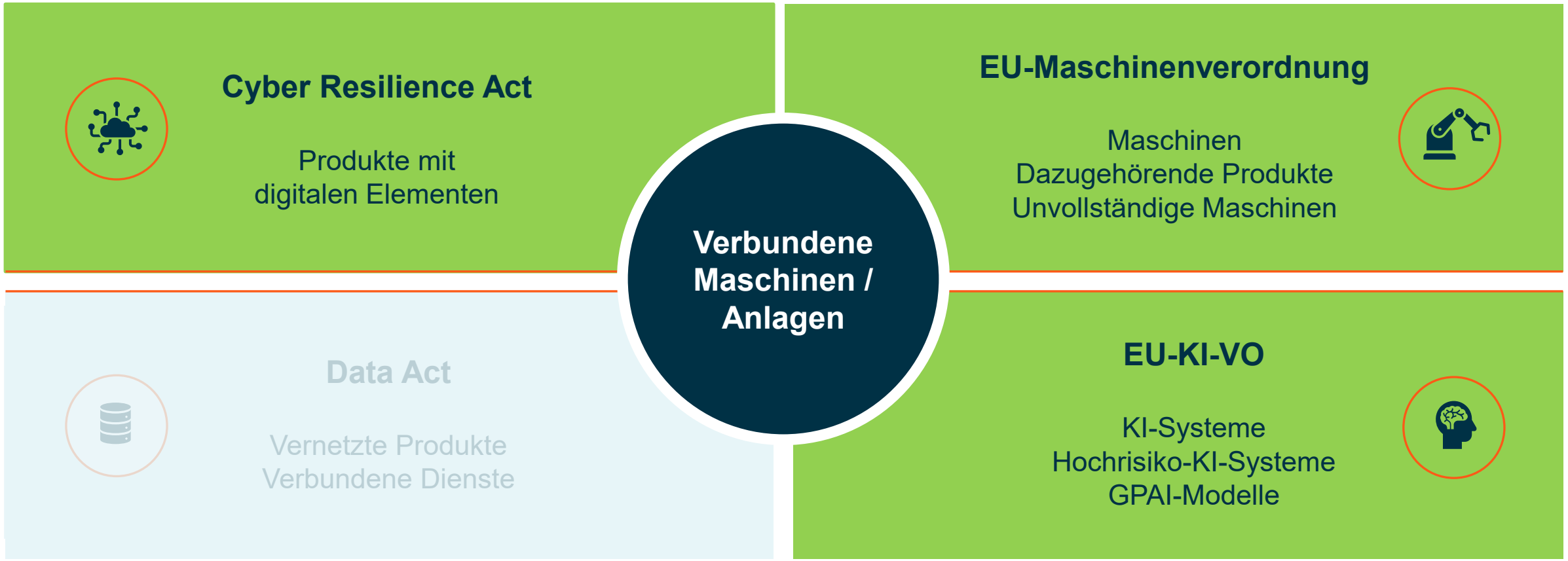
Data Act

Vernetzte Produkte
Verbundene Dienste

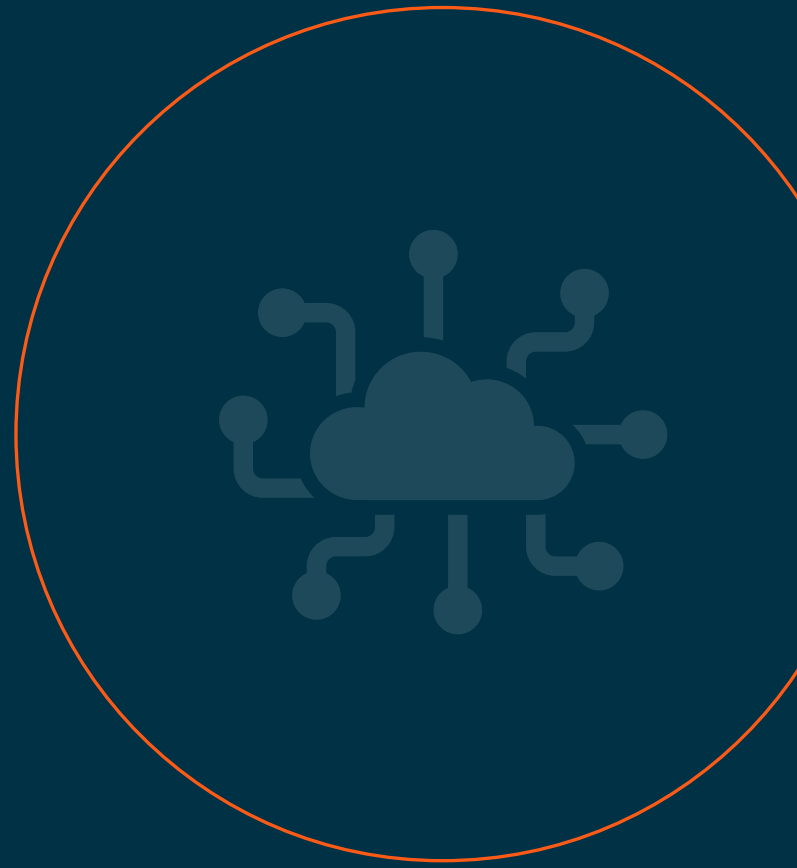
EU-KI-VO

KI-Systeme
Hochrisiko-KI-Systeme
GPAI-Modelle

III. Cybersecurity und KI in Maschinen und Anlagen



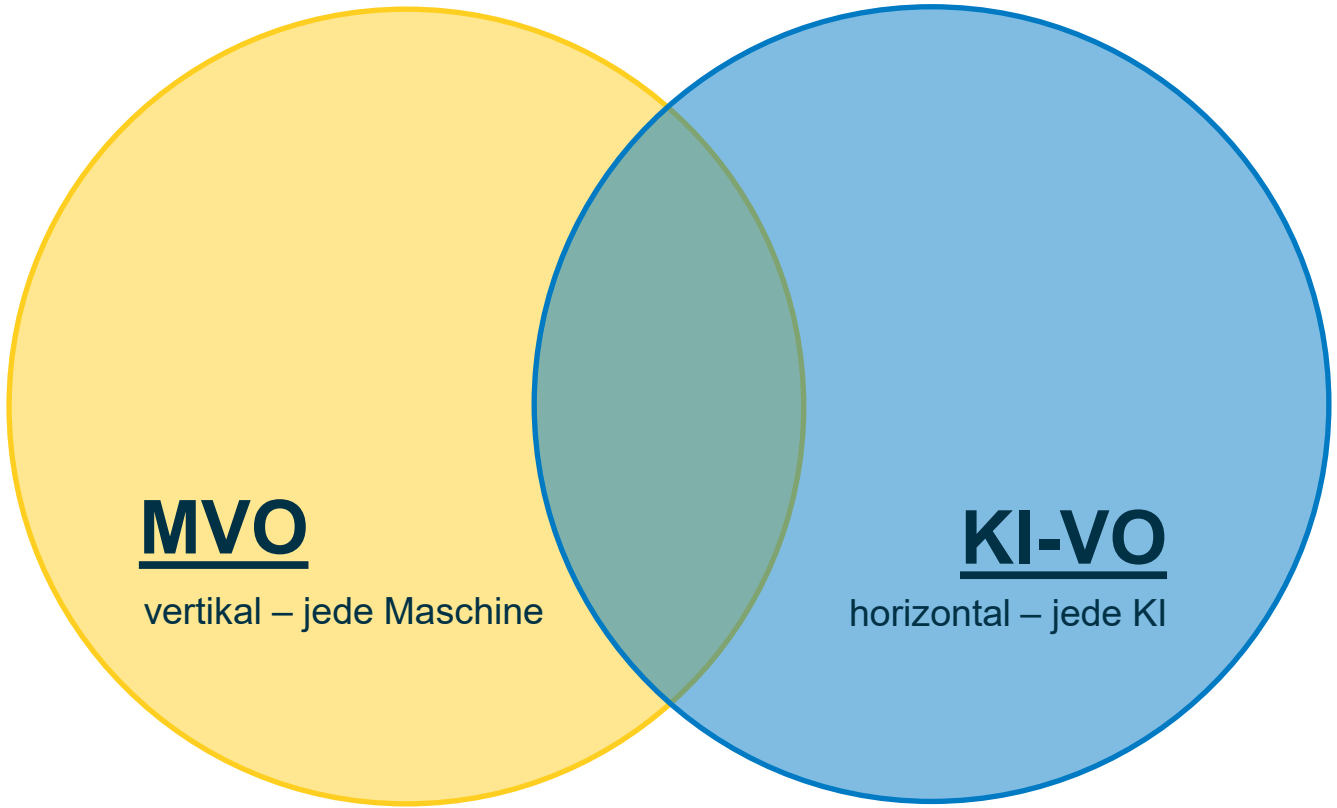
Cyber Resilience Act – In a nutshell



Der **Cyber Resilience Act** legt ein **Mindestmaß an Cybersicherheit für alle vernetzten Produkte** fest, die auf dem EU-Markt erhältlich sind. Ziel ist es, die Cybersicherheit innerhalb der Europäischen Union zu erhöhen.

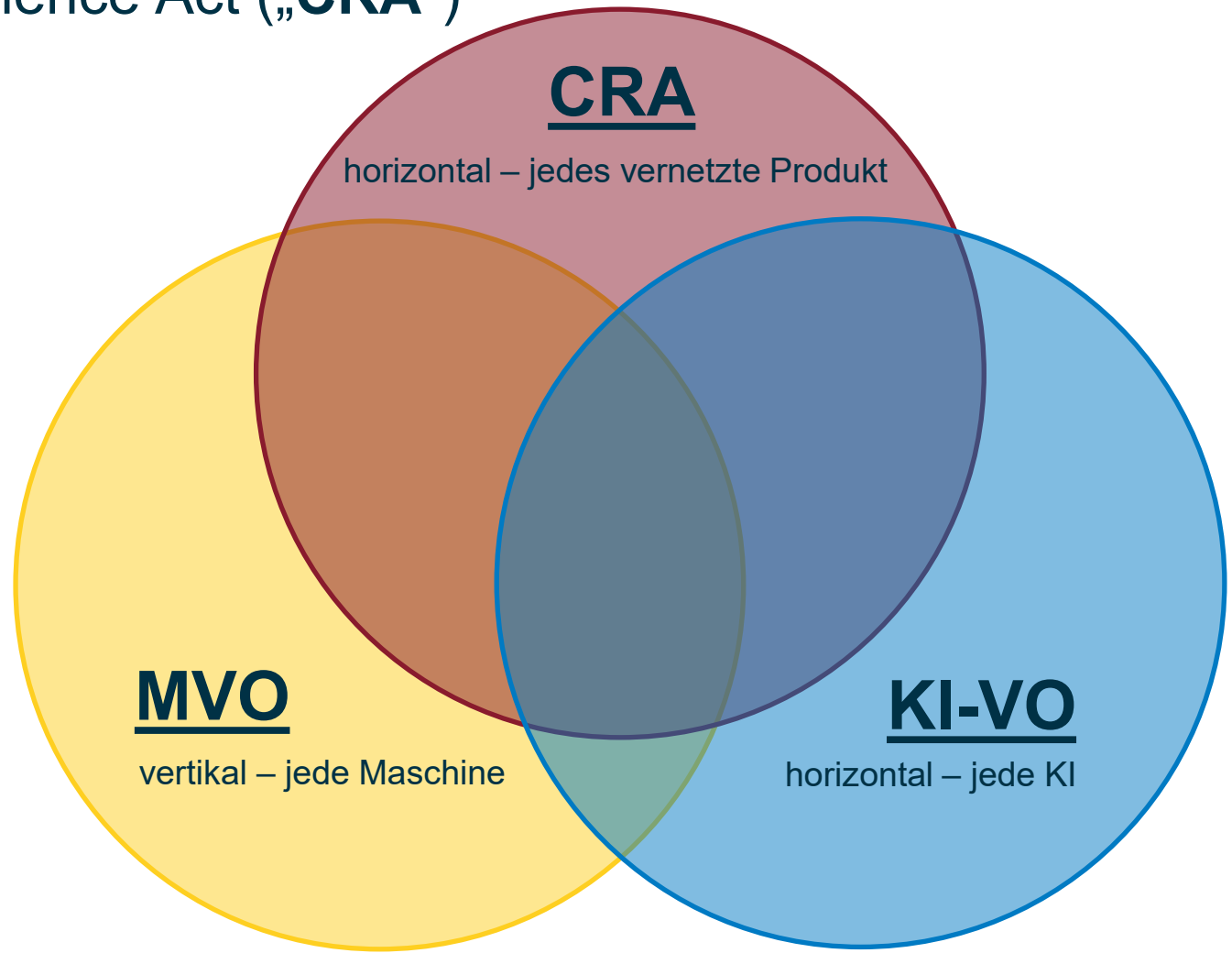
III. Cybersecurity und KI in Maschinen und Anlagen

4. Cyber Resilience Act („**CRA**“)



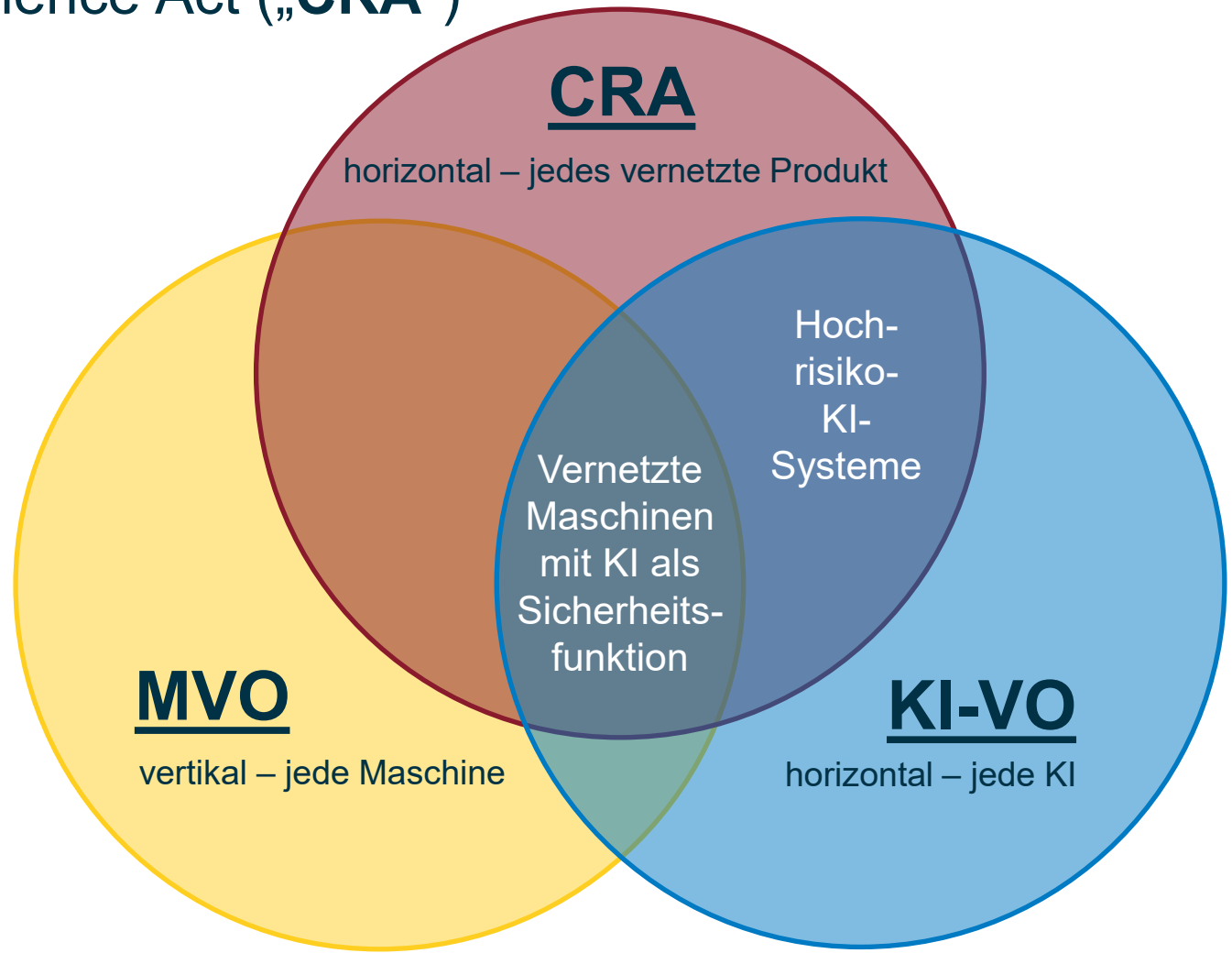
III. Cybersecurity und KI in Maschinen und Anlagen

4. Cyber Resilience Act („**CRA**“)



III. Cybersecurity und KI in Maschinen und Anlagen

4. Cyber Resilience Act („**CRA**“)



III. Cybersecurity und KI in Maschinen und Anlagen

4. Cyber Resilience Act („**CRA**“)

Grundlagen

- Verordnung = ab 11. Dezember 2027 **unmittelbar anwendbar**
- Allgemeine Sicherheitsanforderungen an Produkte mit digitalen Elementen
  - Umfassender Rahmen von **Entwicklung über den gesamten Lebenszyklus**
  - Einschließlich interner Prozesse beim Hersteller (allgemeine Compliance)
- Wesentlicher Inhalt ähnlich zur Struktur der MVO (Anhang I):
  - Grundlegende **Cybersicherheitsanforderungen** (*Teil I*)
  - Behandlung von **Schwachstellen** (*Teil II*)

III. Cybersecurity und KI in Maschinen und Anlagen

4. Cyber Resilience Act („**CRA**“)

Basics der Cybersecurity (Anhang I, Teil I + Art. 13, 14 CRA)

- **Vollständige Risikobewertung** in der Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase
  - Sicherheitsrisiken **minimieren**
  - Sicherheitsvorfälle **verhindern**
  - Auswirkungen auf Gesundheit und Sicherheit der Nutzer so **gering wie möglich** halten
- **Kontrollmechanismus** zum Schutz vor unbefugtem Zugriff (inkl. deren Meldung)
- Verfügbarkeit wesentlicher/grundlegender Funktionen muss immer gewährleistet sein
- CRA ist **risikobasiert**: Nicht jede Maschine muss zwingend alle Anforderungen erfüllen
- **Mindestens 5 Jahre** nach Inverkehrbringen Sicherheitsupdates, Fixes, etc.
- Beobachtung: Mitteilungspflichten nach aktiv ausgenutzter Schwachstelle (24h / 72h / 14 Tage)

III. Cybersecurity und KI in Maschinen und Anlagen

4. Cyber Resilience Act („**CRA**“)

Überschneidungen bei Hochrisiko-KI-Systemen

- Gleichzeitige Erfassung durch **MVO**, **KI-VO** und **CRA**
- Erwägungsgründe KI-VO / CRA: **Konformität** mit Cybersicherheitsanforderungen der **KI-VO** wird erreicht **durch Einhaltung der CRA-Voraussetzungen** und Nachweis in Konformitätserklärung
  - CRA-Compliance ersetzt KI-VO hinsichtlich **Cybersicherheit**
  - KI-VO weiterhin bzgl. Integrität, funktionale Sicherheit, Vertrauenswürdigkeit der **KI**
- Hochrisiko-KI-System: **Konformitätsbewertungsverfahren** richtet sich nach KI-VO
  - KI-VO richtet sich **nach MVO** (aber Besonderheiten **KI-VO/CRA berücksichtigen**)

IV. Exkurs: Ausweitung der Produkthaftung

IV. Exkurs: Ausweitung der Produkthaftung

Die neue EU-Produkthaftungsrichtlinie

- Grundlage des deutschen Produkthaftungsgesetzes (**ProdHaftG**), Inkrafttreten wohl im Laufe des Jahres 2026 (noch im parlamentarischen Verfahren)
- Schäden durch fehlerhafte Produkte („Gefährdungshaftung“ = **verschuldensunabhängig**)
- Neu: Lieferant und Hersteller haften **parallel** (statt nachrangig)
- Software/KI-Systeme als „**Produkt**“, mangelhafte Cybersecurity als „**Fehler**“
- *„Produkt ist **fehlerhaft, wenn es nicht die Sicherheit bietet, die** nach deutschem Recht oder **nach dem Recht der Europäischen Union vorgeschrieben ist** oder die erwartet werden darf.“*
- Beurteilung der Fehlerhaftigkeit u.a.: **Produktsicherheit-/Cybersicherheitsanforderungen**
- „Plausibler Anspruch“: Hersteller muss **relevante Beweismittel offenlegen**

V. Auswirkungen auf die formelle Konformität

V. Auswirkungen auf die formelle Konformität

1. Implikationen der CE-Kennzeichnung

- **MVO**, **KI-VO** und **CRA** sehen jeweils eine CE-Kennzeichnung vor
- Allgemeiner Grundsatz: Hersteller gibt durch das Anbringen der CE-Kennzeichnung an, dass er die **Verantwortung für die Konformität** eines Produktes mit **allen** in den einschlägigen Harmonisierungsrechtsvorschriften enthaltenen Anforderungen **übernimmt**
- Interne Product Compliance: Umfassende Bewertung aller einschlägigen Vorschriften **essenziell**
  - ➢ Verkennen von KI-VO oder CRA kann **weitreichende Folgen** haben (Eingreifen von Marktüberwachungsbehörden, Sanktionen wie Bußgeld, Strafbarkeit)

V. Auswirkungen auf die formelle Konformität

2. EU-Konformitäts- und Einbauerklärung

- **MVO**, **KI-VO** und **CRA** sehen jeweils **Konformitätserklärungen** vor
- Gelten mehrere Harmonisierungsrechtsvorschriften, muss der Hersteller **eine einzige Konformitätserklärung** in Bezug auf alle einschlägigen Vorschriften vorlegen
- **Einbauerklärung** nur in MVO
  - Unvollständige Maschinen könnten aber im Sinne von **KI-VO / CRA „vollständig“** sein
  - Zusätzliche Konformitätserklärung nach KI-VO und CRA erforderlich
  - Einbauerklärung muss **Satz enthalten**, in dem die **Konformität** mit den anderen Rechtsakten erklärt wird (Art. 22 Abs. 3 MVO + Anhang V, Teil B, Ziff. 5 MVO)

V. Auswirkungen auf die formelle Konformität

3. Digitalisierung

- MVO, KI-VO und CRA ermöglichen eine umfangreiche Digitalisierung
  - Möglichkeit zur Bereitstellung **digitaler Betriebsanleitungen**
  - Freiwillige **digitale EU-Konformitätserklärungen**
- **Problem:** Nicht alle Harmonisierungsvorschriften sind EU-Verordnungen
  - Teilweise nationale **Umsetzung in deutsches Recht erforderlich**
  - Viele deutsche Vorschriften sehen noch keine (ausdrückliche) Digitalisierung vor
  - Selbst ProdSG / EU-GPSR verlangen **Dokumente in verkörperter Form** *(umstr.)*

V. Auswirkungen auf die formelle Konformität

3. Digitalisierung

- Reformvorschlag der EU durch **Omnibus-IV-Paket**
  - EU-Konformitätserklärungen **ausschließlich** in elektronischer Form
  - Betriebsanleitungen elektronisch **möglich**, soweit Papierversion angefordert werden kann
  - Omnibus-IV-Paket **ist EU-Richtlinie**, soweit Harmonisierungsvorschriften EU-Richtlinien sind
    - Tätigwerden des deutschen Gesetzgebers nötig
    - Entwurf bereits im Bundestag; **Zeitrahmen allerdings unklar**
- Risiko: Rechtsunsicherheit im Übergangszeitraum
  - Maschine fällt ggf. unter mehrere Vorschriften; teils „digitalisiert“ - teils analog
  - Rechtsauffassung der zuständigen Behörden **noch nicht abzusehen**
  - Jedenfalls bis nicht unter MVO EU-Konformitätserklärung ausschließlich digital ermöglicht ist, sollte **vorsichtshalber weiterhin** – mindestens auch – **„analog“ ausgeliefert werden**

VI. Fragen?

Vielen Dank
für Ihre Aufmerksamkeit!