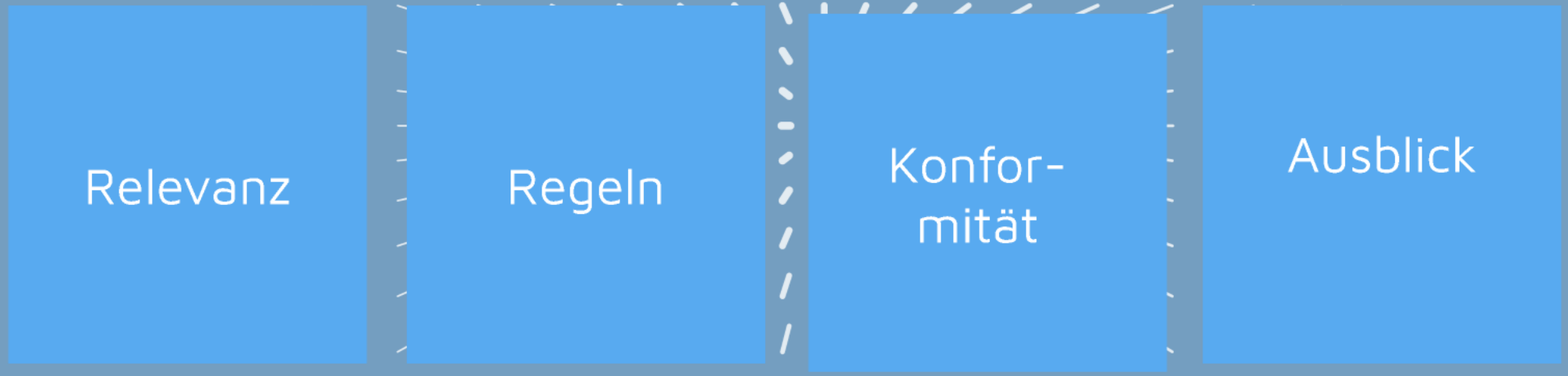
Die KI-Verordnung der Europäischen Unio
Urheberrecht und Datenschutz



Prof. Dr. Christian Djeffal, TUM

Relevanz

Umfassender Rechtsrahmen zur Produktsicherheit (nicht für andere Aspekte) für KI in Europa der folgende Ziele verfolgt

- Förderung einer vertrauenswürdigen KI in Europa
- Schutz der Grundrechte und Sicherheit der Bürger
- Harmonisierung der KI-Regulierung im EU-Binnenmarkt
- Stärkung von Innovation und Wettbewerbsfähigkeit

KI

Sektoren und Anwen-dungen

Akteure in der Wert-schöpfung

Zeit

KI

Art. 3 Nr. 1

- Hebt wesentlich auf Autonomie der Systeme ab,
- keine Beschreibung der zugrundeliegenden Technologien;
- Machine Learning i.d.R. erfasst

Relevanz

Umfassender Rechtsrahmen zur Produktsicherheit (nicht für andere Aspekte) für KI in Europa der folgende Ziele verfolgt

- Förderung einer vertrauenswürdigen KI in Europa
- Schutz der Grundrechte und Sicherheit der Bürger
- Harmonisierung der KI-Regulierung im EU-Binnenmarkt
- Stärkung von Innovation und Wettbewerbsfähigkeit

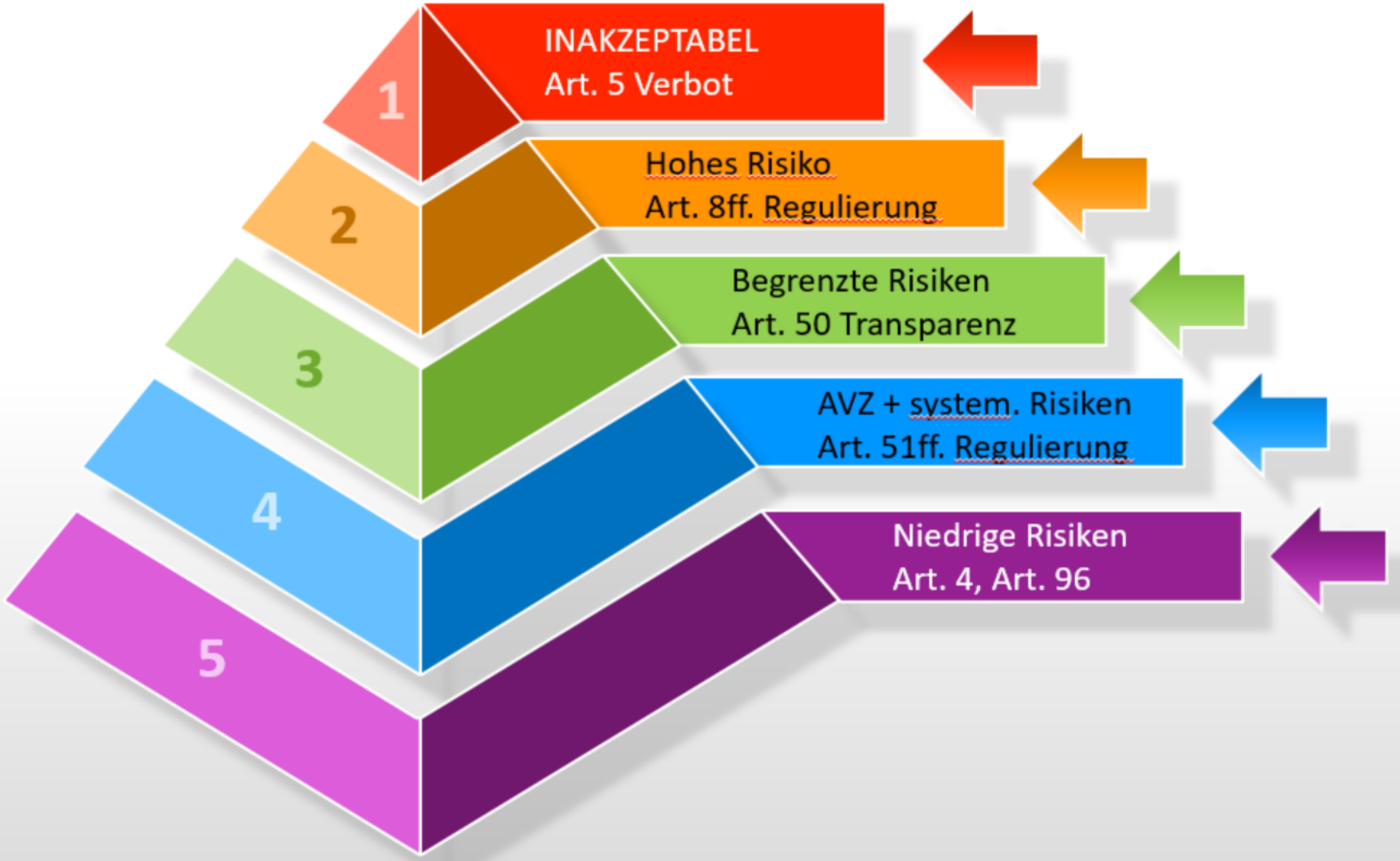
KI

Sektoren und Anwen-dungen

Akteure in der Wert-schöpfung

Zeit

Risiko-basierter Ansatz



Hochrisiko-KI-System?

- Art. 6 Abs. 1: KI ist Sicherheitsbauteil für harmonisiertes Produkt oder Produkt welches einer Konformitätsbewertung durch Dritte unterliegt
- Art. 6 Abs. 2: spezifische Bestimmung in Anhang III

Anhang III

1. Biometrie: KI-Systeme zur biometrischen Fernidentifizierung, Kategorisierung und Emotionserkennung.

2. Kritische Infrastruktur: KI-Systeme zur Sicherheit und Verwaltung von digitaler und öffentlicher Infrastruktur (z.B. Straßenverkehr, Energieversorgung).

3. Allgemeine und berufliche Bildung: KI-Systeme zur Zulassung, Bewertung, Überwachung und Verhaltenskontrolle in Bildungseinrichtungen.

Anhang III

4. Beschäftigung und Personalmanagement: KI-Systeme zur Personalauswahl, Aufgabenverteilung und Leistungsbewertung.

5. Grundlegende Dienste: KI-Systeme zur Beurteilung des Zugangs zu öffentlichen Leistungen, Kreditwürdigkeit und Notfalldienst-Koordination.

6. Strafverfolgung: KI-Systeme zur Risikoeinschätzung, Lügendetektion, Beweisbewertung und Profilierung.

Anhang III

7. Migration und Grenzkontrolle: KI-Systeme zur Risikobewertung, Visumprüfung und Identifikation.

8. Rechtspflege und demokratische Prozesse: KI-Systeme zur Unterstützung der Justiz und zur Beeinflussung von Wahlen oder Referenden.

Relevanz

Umfassender Rechtsrahmen zur Produktsicherheit (nicht für andere Aspekte) für KI in Europa der folgende Ziele verfolgt

- Förderung einer vertrauenswürdigen KI in Europa
- Schutz der Grundrechte und Sicherheit der Bürger
- Harmonisierung der KI-Regulierung im EU-Binnenmarkt
- Stärkung von Innovation und Wettbewerbsfähigkeit

KI

Sektoren und Anwen-dungen

Akteure in der Wert-schöpfung

Zeit

Rollen in der Entwicklung

Definition der Rollen im KI-Systemsektor.

ANBIETER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;

BETREIBER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

BEVOLLMÄCHTIGTER

Eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;

EINFÜHRER

eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt;
„Händler": eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;

Rollen in der Entwicklung

Definition der Rollen im KI-Systemsektor.

ANBIETER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;

BETREIBER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

BEVOLLMÄCHTIGTER

Eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;

EINFÜHRER

eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt;
„Händler": eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;

ANBIETER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;

BETREIBER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

BEVOLLMÄCHTIGTER

Eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;

EINFÜHRER

eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt;

„**Händler**“: eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;

Rollen in der Entwicklung

Definition der Rollen im KI-Systemsektor.

ANBIETER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;

BETREIBER

eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

BEVOLLMÄCHTIGTER

Eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;

EINFÜHRER

eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt;
„Händler": eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;

Relevanz

Umfassender Rechtsrahmen zur Produktsicherheit (nicht für andere Aspekte) für KI in Europa der folgende Ziele verfolgt

- Förderung einer vertrauenswürdigen KI in Europa
- Schutz der Grundrechte und Sicherheit der Bürger
- Harmonisierung der KI-Regulierung im EU-Binnenmarkt
- Stärkung von Innovation und Wettbewerbsfähigkeit

KI

Sektoren und Anwen-dungen

Akteure in der Wert-schöpfung

Zeit

Wichtige Fristen

- 2. Feb 2025: Verbot bestimmter „unannehmbarer“ KI-Systeme, Start der Bildungsanforderungen für Anbieter und Betreiber
- 2. Aug 2025: Pflichten für General-Purpose-KI und Strafvorschriften werden aktiv
- 2. Aug 2026: Vollständige Anwendung der meisten Verordnungspunkte
- 2. Aug 2027: Hochrisiko-KI-Regelungen gemäß Artikel 6(1)

Relevanz

Umfassender Rechtsrahmen zur Produktsicherheit (nicht für andere Aspekte) für KI in Europa der folgende Ziele verfolgt

- Förderung einer vertrauenswürdigen KI in Europa
- Schutz der Grundrechte und Sicherheit der Bürger
- Harmonisierung der KI-Regulierung im EU-Binnenmarkt
- Stärkung von Innovation und Wettbewerbsfähigkeit

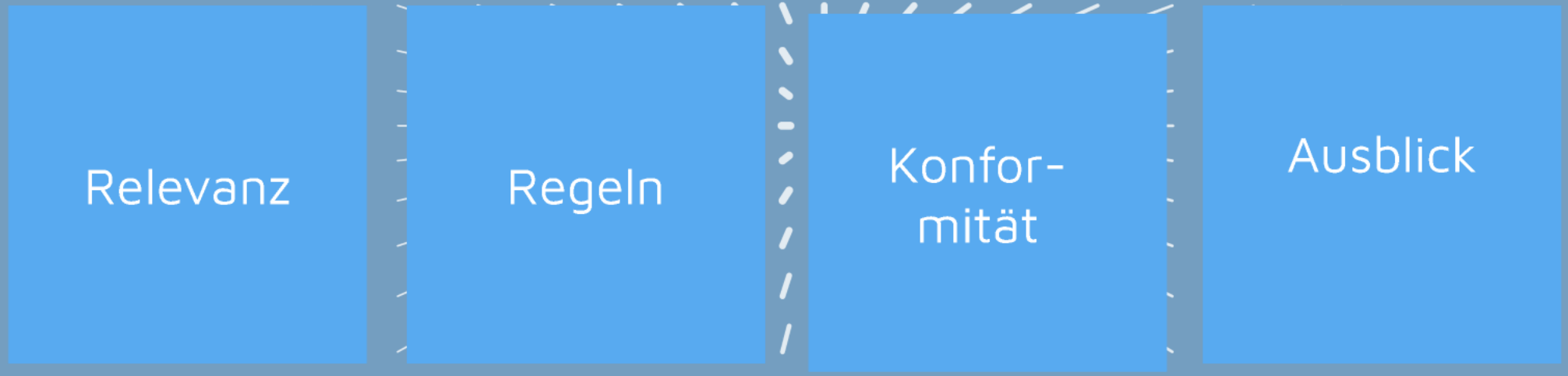
KI

Sektoren und Anwen-dungen

Akteure in der Wert-schöpfung

Zeit

Die KI-Verordnung der Europäischen Unio
Urheberrecht und Datenschutz



Prof. Dr. Christian Djeffal, TUM

Regeln

Was ist geregelt?
- KI VO enthält offene Anforderungen
- Sie etabliert ferner Prozesse in den betreffenden Organisationen

Risiko-
managem
ent

Anforderungen

RISIKOMANAGEMENTSYSTEM

Wichtige Schritte und Anforderungen des Risikomanagementsystems gemäß dem AI Act.

RISIKOERMITTLUNG

RISIKOBEWERTUNG

MASSNAHMEN

Kontrolle Anforderungen

RISIKOMANAGEMENTSYSTEM

Wichtige Schritte und Anforderungen des Risikomanagementsystems gemäß dem AI Act.

RISIKOERMITTLUNG

Identifikation bekannter und vorhersehbarer Risiken mit einem Fokus auf Gesundheit, Sicherheit und Grundrechte, insbesondere unter Berücksichtigung der bestimmungsgemäßen Verwendung.

RISIKOBEWERTUNG

Analyse der bestimmungsgemäßen Verwendung sowie Bewertung möglicher Fehlanwendungen, die durch Marktbeobachtungsdaten unterstützt wird.

MASSNAHMEN

Implementierung gezielter Gegenmaßnahmen zur Bewertung von Wechselwirkungen und Sicherstellung von vertretbaren Restrisiken.

Zentrale Anforderungen:

- Dokumentationspflicht
- Regelmäßige Überprüfung/Aktualisierung
- Tests zur Validierung
- Schutz vulnerabler Gruppen (bes. unter 18 Jahren)
- Integration in existierende Prozesse möglich

RISIKOERMITTLUNG

Identifikation bekannter und vorhersehbarer Risiken mit einem Fokus auf Gesundheit, Sicherheit und Grundrechte, insbesondere unter Berücksichtigung der bestimmungsgemäßen Verwendung.

RISIKOBEWERTUNG

Analyse der bestimmungsgemäßen Verwendung sowie Bewertung möglicher Fehlanwendungen, die durch Marktbeobachtungsdaten unterstützt wird.

MASSNAHMEN

Implementierung gezielter Gegenmaßnahmen zur Bewertung von Wechselwirkungen und Sicherstellung von vertretbaren Restrisiken.

Zentrale Anforderungen:

- Dokumentationspflicht
- Regelmäßige Überprüfung/Aktualisierung
- Tests zur Validierung
- Schutz vulnerabler Gruppen (bes. unter 18 Jahren)
- Integration in existierende Prozesse möglich

RISIKOMANAGEMENTSYSTEM

Wichtige Schritte und Anforderungen des Risikomanagementsystems gemäß dem AI Act.

RISIKOERMITTLUNG

Identifikation bekannter und vorhersehbarer Risiken mit einem Fokus auf Gesundheit, Sicherheit und Grundrechte, insbesondere unter Berücksichtigung der bestimmungsgemäßen Verwendung.

RISIKOBEWERTUNG

Analyse der bestimmungsgemäßen Verwendung sowie Bewertung möglicher Fehlanwendungen, die durch Marktbeobachtungsdaten unterstützt wird.

MASSNAHMEN

Implementierung gezielter Gegenmaßnahmen zur Bewertung von Wechselwirkungen und Sicherstellung von vertretbaren Restrisiken.

Zentrale Anforderungen:

- Dokumentationspflicht
- Regelmäßige Überprüfung/Aktualisierung
- Tests zur Validierung
- Schutz vulnerabler Gruppen (bes. unter 18 Jahren)
- Integration in existierende Prozesse möglich

Regeln

Was ist geregelt?
- KI VO enthält offene Anforderungen
- Sie etabliert ferner Prozesse in den betreffenden Organisationen

Risiko-
managem
ent

Anforderungen

DATEN UND KI-GOVERNANCE

Bestimmungen zur Sicherstellung von Datenqualität und Dokumentation in Hochrisiko-KI-Systemen.

DATEN UND DATEN-GOVERNANCE

Hochrisiko-KI-Systeme müssen mit qualitativ hochwertigen Trainings-, Validierungs- und Testdatensätzen entwickelt werden. Diese müssen durch geeignete Datenmanagementverfahren verwaltet und auf Verzerrungen überprüft werden.

TECHNISCHE DOKUMENTATION

Die technische Dokumentation muss vor dem Inverkehrbringen des Systems erstellt werden und nachweisen, dass alle Anforderungen erfüllt sind, wobei vereinfachte Dokumentationsformen für KMUs möglich sind.

AUFZEICHNUNGSPFLICHTEN

Die Systeme müssen eine automatische Protokollierung von Ereignissen während ihres gesamten Lebenszyklus ermöglichen, um die Rückverfolgbarkeit des Betriebs zu gewährleisten.

TRANSPARENZ UND AUFSICHT

Die Regulierung moderner Hochrisiko-KI-Systeme erfordert Transparenz und menschliche Aufsicht.

TRANSPARENZ

Hochrisiko-KI-Systeme müssen für Nutzer so transparent sein, und es sind Betriebsanleitungen bieten, die wesentliche Informationen über ihre Leistungsgrenzen und korrekte Nutzung enthalten.

MENSCHLICHE AUFSICHT

Diese Systeme müssen so gestaltet sein, dass Menschen effektiv die Kontrolle ausüben können, inklusive der Option, das System zu stoppen oder einzugreifen.

SYSTEMANFORDERUNGEN

Wichtige Anforderungen für Systemsicherheit und Stabilität.

GENAUIGKEIT

ROBUSTHEIT

CYBERSICHERHEIT

SYSTEMANFORDERUNGEN

Wichtige Anforderungen für Systemsicherheit und Stabilität.

GENAUIGKEIT

Die Systeme müssen ein angemessenes Maß an Genauigkeit erreichen und während ihres gesamten Lebenszyklus beständig funktionieren.

ROBUSTHEIT

Die Systeme müssen widerstandsfähig gegen Fehler, Störungen und Unstimmigkeiten sein und können dies durch technische Redundanz erreichen.

CYBERSICHERHEIT

Die Systeme müssen gegen unbefugte Zugriffe und Manipulationsversuche geschützt sein, insbesondere gegen KI-spezifische Angriffe wie "data poisoning" oder "adversarial examples".

GENAUIGKEIT

Die Systeme müssen ein angemessenes Maß an Genauigkeit erreichen und während ihres gesamten Lebenszyklus beständig funktionieren.

ROBUSTHEIT

Die Systeme müssen widerstandsfähig gegen Fehler, Störungen und Unstimmigkeiten sein und können dies durch technische Redundanz erreichen.

CYBERSICHERHEIT

Die Systeme müssen gegen unbefugte Zugriffe und Manipulationsversuche geschützt sein, insbesondere gegen KI-spezifische Angriffe wie "data poisoning" oder "adversarial examples".

SYSTEMANFORDERUNGEN

Wichtige Anforderungen für Systemsicherheit und Stabilität.

GENAUIGKEIT

Die Systeme müssen ein angemessenes Maß an Genauigkeit erreichen und während ihres gesamten Lebenszyklus beständig funktionieren.

ROBUSTHEIT

Die Systeme müssen widerstandsfähig gegen Fehler, Störungen und Unstimmigkeiten sein und können dies durch technische Redundanz erreichen.

CYBERSICHERHEIT

Die Systeme müssen gegen unbefugte Zugriffe und Manipulationsversuche geschützt sein, insbesondere gegen KI-spezifische Angriffe wie "data poisoning" oder "adversarial examples".

TRANSPARENZ UND AUFSICHT

Die Regulierung moderner Hochrisiko-KI-Systeme erfordert Transparenz und menschliche Aufsicht.

TRANSPARENZ

Hochrisiko-KI-Systeme müssen für Betreiber transparent sein und klare Betriebsanleitungen bieten, die wesentliche Informationen über ihre Leistungsgrenzen und korrekte Nutzung enthalten.

MENSCHLICHE AUFSICHT

Diese Systeme müssen so gestaltet sein, dass Menschen effektiv die Kontrolle ausüben können, inklusive der Option, das System zu stoppen oder einzugreifen.

SYSTEMANFORDERUNG

Wichtige Anforderungen für Systemsicherheit und Stabilität.

GENAUIGKEIT

ROBUSTHEIT

TRANSPARENZ

Hochrisiko-KI-Systeme müssen für Betreiber transparent sein und klare Betriebsanleitungen bieten, die wesentliche Informationen über ihre Leistungsgrenzen und korrekte Nutzung enthalten.

MENSCHLICHE AUFSICHT

Diese Systeme müssen so gestaltet sein, dass Menschen effektiv die Kontrolle ausüben können, inklusive der Option, das System zu stoppen oder einzugreifen.

TRANSPARENZ UND AUFSICHT

Die Regulierung moderner Hochrisiko-KI-Systeme erfordert Transparenz und menschliche Aufsicht.

TRANSPARENZ

Hochrisiko-KI-Systeme müssen für Betreiber transparent sein und klare Betriebsanleitungen bieten, die wesentliche Informationen über ihre Leistungsgrenzen und korrekte Nutzung enthalten.

MENSCHLICHE AUFSICHT

Diese Systeme müssen so gestaltet sein, dass Menschen effektiv die Kontrolle ausüben können, inklusive der Option, das System zu stoppen oder einzugreifen.

SYSTEMANFORDERUNG

Wichtige Anforderungen für Systemsicherheit und Stabilität.

GENAUIGKEIT

ROBUSTHEIT

DATEN UND KI-GOVERNANCE

Bestimmungen zur Sicherstellung von Datenqualität und Dokumentation in Hochrisiko-KI-Systemen.

DATEN UND DATEN-GOVERNANCE

Hochrisiko-KI-Systeme müssen mit qualitativ hochwertigen Trainings-, Validierungs- und Testdatensätzen entwickelt werden. Diese müssen durch geeignete Datenmanagementverfahren verwaltet und auf Verzerrungen überprüft werden.

TECHNISCHE DOKUMENTATION

Die technische Dokumentation muss vor dem Inverkehrbringen des Systems erstellt werden und nachweisen, dass alle Anforderungen erfüllt sind, wobei vereinfachte Dokumentationsformen für KMUs möglich sind.

AUFZEICHNUNGSPFLICHTEN

Die Systeme müssen eine automatische Protokollierung von Ereignissen während ihres gesamten Lebenszyklus ermöglichen, um die Rückverfolgbarkeit des Betriebs zu gewährleisten.

DATEN UND DATEN-GOVERNANCE

Hochrisiko-KI-Systeme müssen mit qualitativ hochwertigen Trainings-, Validierungs- und Testdatensätzen entwickelt werden. Diese müssen durch geeignete Datenmanagementverfahren verwaltet und auf Verzerrungen überprüft werden.

TECHNISCHE DOKUMENTATION

Die technische Dokumentation muss vor dem Inverkehrbringen des Systems erstellt werden und nachweisen, dass alle Anforderungen erfüllt sind, wobei vereinfachte Dokumentationsformen für KMUs möglich sind.

AUFZEICHNUNGSPFLICHTEN

Die Systeme müssen eine automatische Protokollierung von Ereignissen während ihres gesamten Lebenszyklus ermöglichen, um die Rückverfolgbarkeit des Betriebs zu gewährleisten.

DATEN UND KI-GOVERNANCE

Bestimmungen zur Sicherstellung von Datenqualität und Dokumentation in Hochrisiko-KI-Systemen.

DATEN UND DATEN-GOVERNANCE

Hochrisiko-KI-Systeme müssen mit qualitativ hochwertigen Trainings-, Validierungs- und Testdatensätzen entwickelt werden. Diese müssen durch geeignete Datenmanagementverfahren verwaltet und auf Verzerrungen überprüft werden.

TECHNISCHE DOKUMENTATION

Die technische Dokumentation muss vor dem Inverkehrbringen des Systems erstellt werden und nachweisen, dass alle Anforderungen erfüllt sind, wobei vereinfachte Dokumentationsformen für KMUs möglich sind.

AUFZEICHNUNGSPFLICHTEN

Die Systeme müssen eine automatische Protokollierung von Ereignissen während ihres gesamten Lebenszyklus ermöglichen, um die Rückverfolgbarkeit des Betriebs zu gewährleisten.

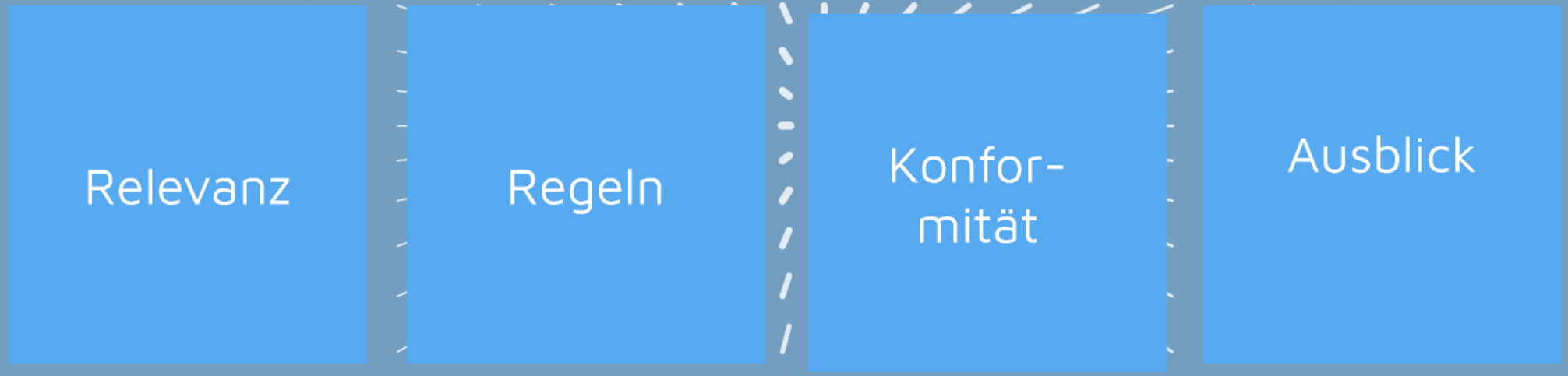
Regeln

Was ist geregelt?
- KI VO enthält offene Anforderungen
- Sie etabliert ferner Prozesse in den betreffenden Organisationen

Risiko-
managem
ent

Anforderungen

Die KI-Verordnung der Europäischen Unio
Urheberrecht und Datenschutz



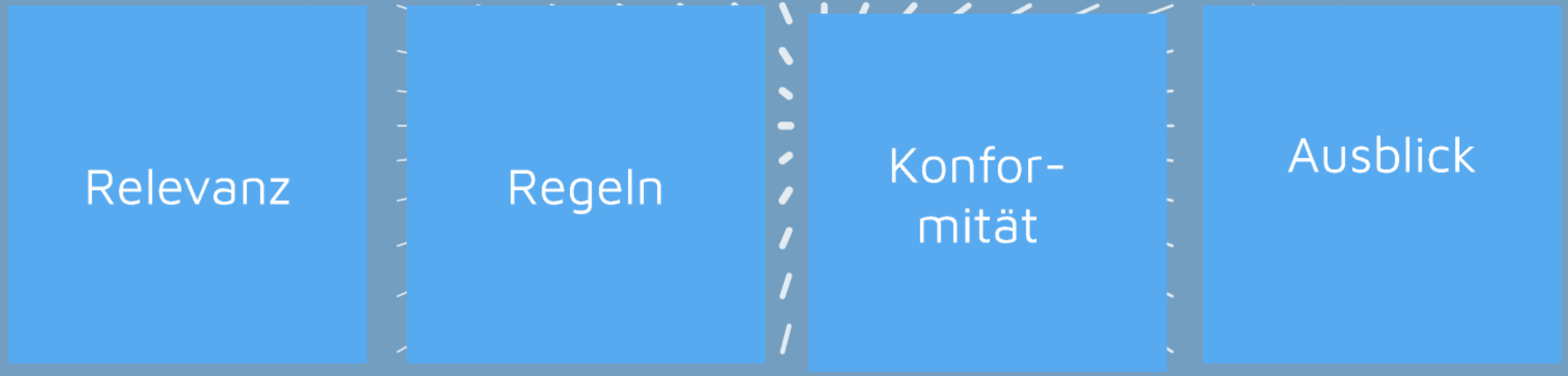
Prof. Dr. Christian Djeffal, TUM

Konformitäts-bewertung

Zentrale Bausteine:

- Harmonisierte Standards sind nicht zwingend zu nutzen und vermitteln nur die Vermutung der Konformität
- Grundsätzlich kann die Konformität innerhalb der Organisation bewertet werden. Es sind keine benannte Stellen erforderlich

Die KI-Verordnung der Europäischen Unio
Urheberrecht und Datenschutz



Prof. Dr. Christian Djeffal, TUM

Ausblick

Wissens-
gover-
nance

Möglich-
keiten

Sonstige
Fragen

Wissensgovernance

Die KI-VO fordert von Orgas selbst Inhalt der Pflichten und Verfahren der Bewertung zu bestimmen

Die KI-VO fordert von Orgas selbst Inhalt der Pflichten und Verfahren der Bewertung zu bestimmen

Wissensgovernance wird zu einer wettbewerbs-relevanten Frage

Zusammenarbeit in Netzwerken ermöglicht Synergieen und entscheidende Vorteile.

Die KI-VO fordert von Orgas selbst Inhalt der Pflichten und Verfahren der Bewertung zu bestimmen

Ausblick

Wissens-
gover-
nance

Möglich-
keiten

Sonstige
Fragen

Möglichkeiten

KI-Büro der Eur. Kommision

Reallabore & Testen unter Realbe-dingungen

Was noch?

Allgemeine Struktur

Das EU AI Office ist Teil der Generaldirektion CNECT und hat fünf Hauptbereiche:

1. Regulierung und Compliance: Einheitliche Umsetzung des AI Acts koordinieren.
2. KI-Sicherheit: Risiken bei KI-Modellen bewerten.
3. Exzellenz in KI & Robotik: Förderung der Forschung und GenAI4EU-Initiative.
4. KI für das Gemeinwohl: Internationale Zusammenarbeit stärken.
5. KI-Innovation: Strategieumsetzung und Unterstützung von Innovationszentren.

Allgemeine Struktur
Das EU AI Office ist Teil der Generaldirektion CNECT und hat fünf Hauptbereiche:
1. Regulierung und Compliance: Einheitliche Umsetzung des AI Acts koordinieren.
2. KI-Sicherheit: Risiken bei KI-Modellen bewerten.
3. Exzellenz in KI & Robotik: Förderung der Forschung und GenAI4EU-Initiative.
4. KI für das Gemeinwohl: Internationale Zusammenarbeit stärken.
5. KI-Innovation: Strategieumsetzung und Unterstützung von Innovationszentren.

Förderung
- KI-Fabriken (AI Factories): Zugang zu Supercomputern und Entwicklungsumgebungen, speziell für Startups und KMUs.
- Förderprogramme: Horizon Europe und Digital Europe Programme für vertrauenswürdige KI-Entwicklung.
- Europäische digitale Innovationszentren (EDIH)
- Test- und Experimentiereinrichtungen
- Entwicklung gemeinsamer Datenräume

Möglichkeiten

KI-Büro der Eur. Kommision

Reallabore & Testen unter Realbe-dingungen

Was noch?

Reallabore und Tests unter Realbedingugnen

1. Reallabore: Pflicht zur Einrichtung für MS, aufhebung der datenschutzrechtlichen Zweckbindung für öffentl. Sicherheit, Gesundheit, Sicherheit von Mobilität und Verkehr, Nachhaltigkeit und öffentliche Verwaltung

2. Rahmen für Testen unter Realbedingungen: Voraussetzungen werden definiert

Möglichkeiten

KI-Büro der Eur. Kommision

Reallabore & Testen unter Realbe-dingungen

Was noch?

Wie könnten Sie KI noch zur Entwicklung Ihres Unternehmens nutzen?

Beispiel: Art. 4: KI-Kompetenz

Möglichkeit, Mitarbeitende in Management und Büro mit Prompt Engineering und Design in Berührung zu bringen und dabei wichtige Fragen von Datenschutz bis Urheberrecht zu vermitteln.

Möglichkeiten

KI-Büro der Eur. Kommision

Reallabore & Testen unter Realbe-dingungen

Was noch?

Ausblick

Wissens-
gover-
nance

Möglich-
keiten

Sonstige
Fragen

Fragen

- Was bedeutet die Pflicht aus Art. 4 für meine Organisation?
- Verletze ich geistiges Eigentum durch den Einsatz von KI?
- Wie schütze ich kreative Erzeugnisse mit KI?
- Wie gewährleiste ich den datenschutzkonformen Einsatz von KI in meinem Unternehmen?

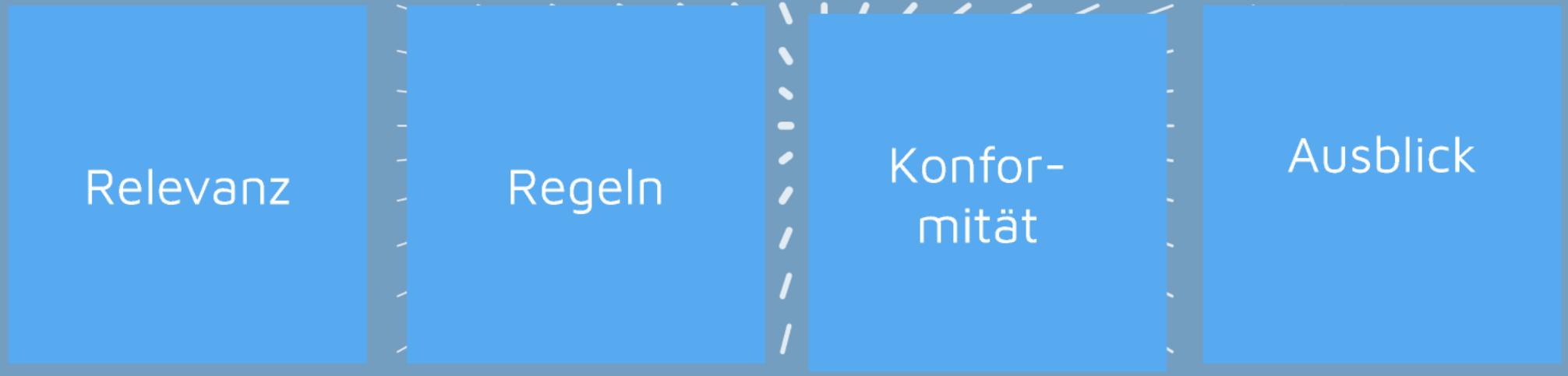
Ausblick

Wissens-
gover-
nance

Möglich-
keiten

Sonstige
Fragen

Die KI-Verordnung der Europäischen Unio
Urheberrecht und Datenschutz



Prof. Dr. Christian Djeffal, TUM