

DEN  
deutsches forschungsnetz

---

---

---



# Die KI-VO und Compliance-Anforderungen für die deutsche Hochschullandschaft

DFN-Konferenz Datenschutz | 09.12.2025

Philipp Schöbel



1. Konzeption der KI-VO
  1. Begriffe und Akteure
  2. Ausnahmen
2. Verbotene KI
3. Hochrisiko-KI
4. KI mit beschränktem Risiko
5. KI-Aufsicht in Deutschland

# DFN

## Konzeption der KI-VO



# Konzeption der KI-Verordnung (KI-VO)

## KI-Systeme

Verbote (Art. 5)

Hochrisiko-KI (Art. 6 ff.)

Transparenzpflichten (Art. 50)

Geringes Risiko (Art. 4)

## KI-Modelle

Allgemeiner  
Verwendungszweck (Art. 51)

Systemisches Risiko (Art. 55)

# Was ist ein KI-System?

Art. 3 Nr. 1 K-VO

1. Ein maschinengestütztes System
2. grundsätzlich für einen autonomen Betrieb ausgelegt
3. kann nach Betriebsaufnahme anpassungsfähig sein
4. leitet (eigenständig) aus Eingaben ab, wie Ausgaben erstellt werden
5. Ausgaben können die physische oder virtuelle Umgebung beeinflussen

# Was ist ein KI-System?

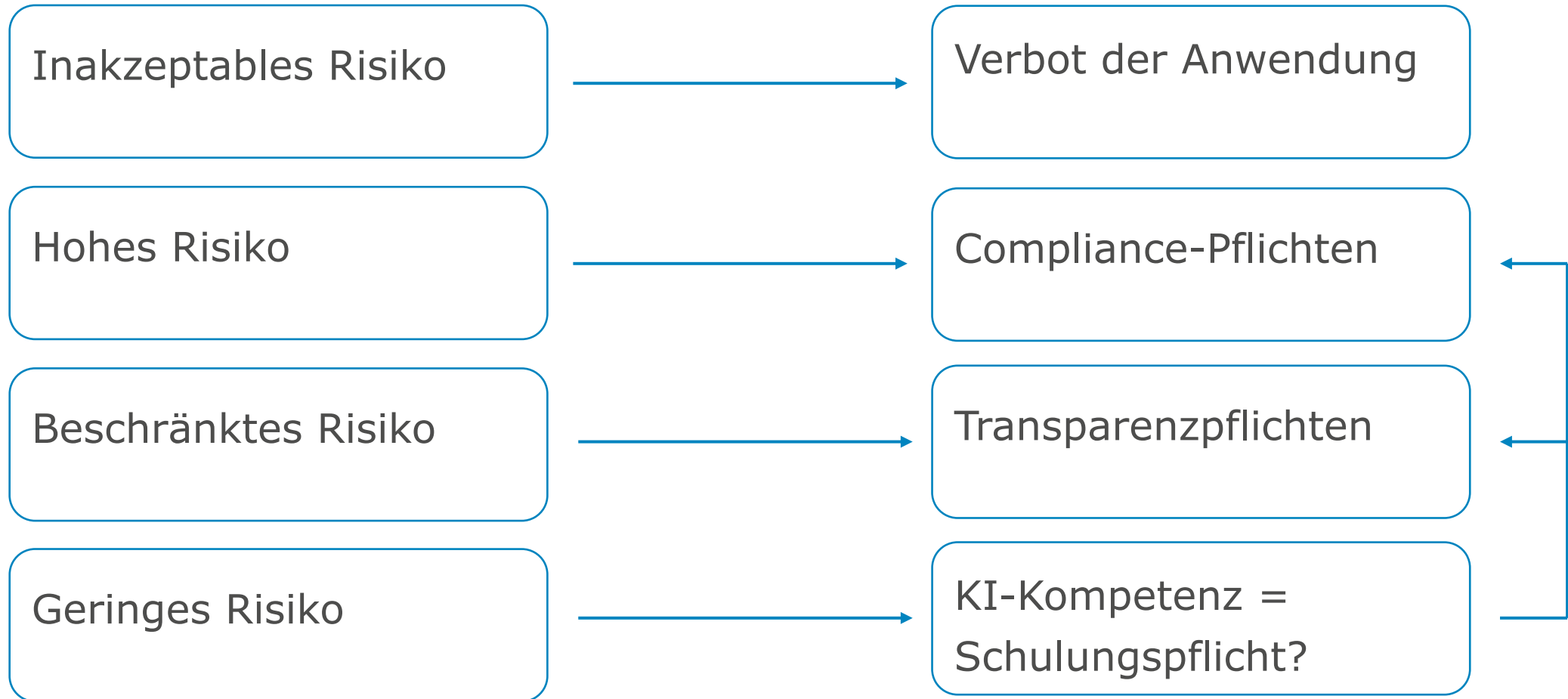
## Autonomer Betrieb

Autonomie bedeutet: KI-Systeme agieren **bis zu einem gewissen Grad** unabhängig von menschlichem Zutun und sind in der Lage, ohne menschliches Eingreifen zu arbeiten. Nicht erfasst sind ausschließlich von natürlichen Personen definierte Regeln für das automatische Ausführen von Operationen.

## Ableiten

Ableiten geht über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden. Dazu gehören Ansätze für maschinelles Lernen, sowie logik- und wissensgestützte Konzepte.

# Risikogruppen für KI-Systeme





# KI-Kompetenz

Fähigkeiten

Kenntnisse

Verständnis

Sachkundiger Einsatz



Bewusstsein für  
Chancen und Risiken



# Ausnahmen für die Wissenschaft

Forschung **an** KI (Art. 2  
Abs. 8 KI-VO)



KI-VO gilt **nicht** für für  
Forschungs-, Test- und  
Entwicklungstätigkeiten zu KI



**Ausnahme:** Tests unter  
Realbedingungen

Forschung **mit** KI (Art. 2  
Abs. 6 KI-VO)



KI-VO gilt **nicht** für KI, die  
ausschließlich für Forschung in  
Betrieb genommen wird

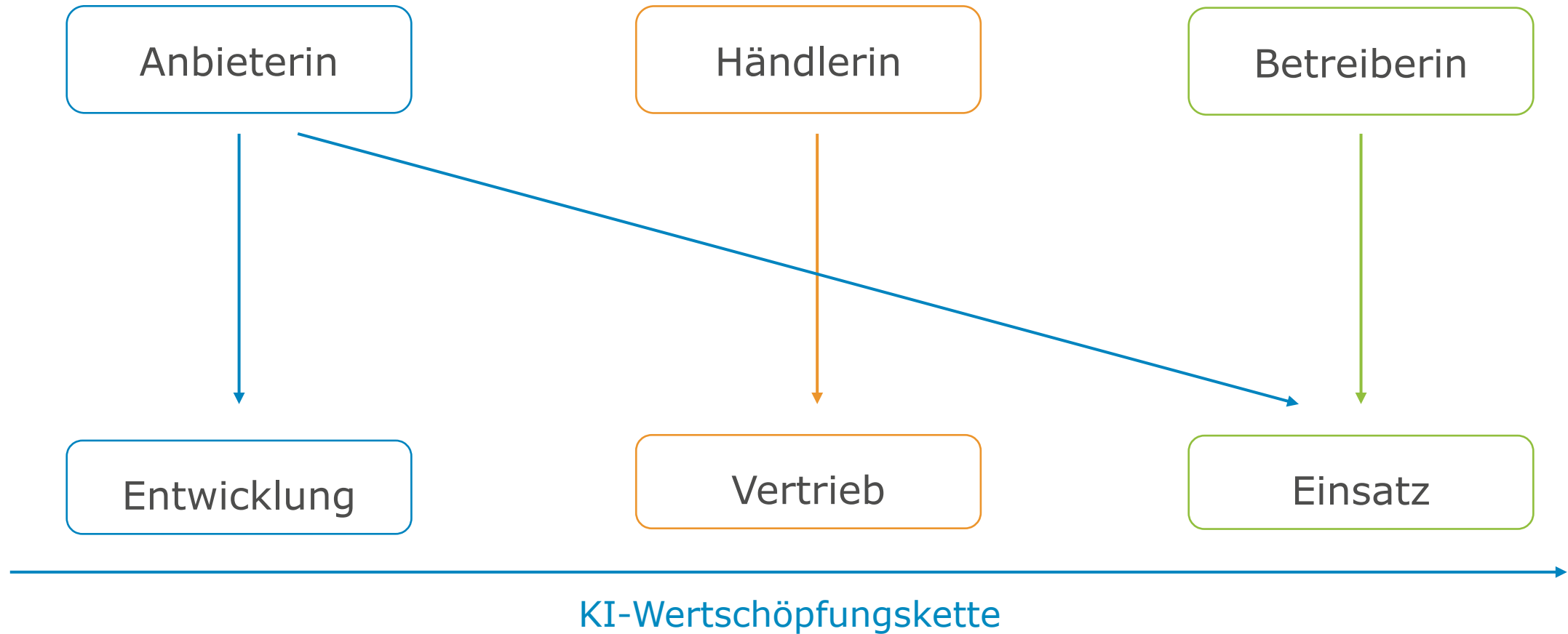
# Ausnahmen für die Wissenschaft

KI-VO gilt **nicht** für KI, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen wird (Art. 2 Abs. 6 KI-VO).

KI-VO gilt für  
Verwaltungstätigkeiten an  
Hochschulen

KI-VO gilt für  
Lehrtätigkeiten an  
Hochschulen

Ausnahme gilt nicht für  
dual-use (z.B. Forschung  
und Lehre)



# Pflichten von Anbieterin und Betreiberin von Hochrisiko-KI-Systemen



Anbieterin

Art. 8,  
Art. 9,  
Art. 10,  
Art. 11,  
Art. 12,  
Art. 13,  
Art. 14,  
Art. 15,  
Art. 16,  
Art. 17,  
Art. 18,  
Art. 19,  
Art. 20,  
Art. 21,  
Art. 22,  
Art. 47-49



Betreiberin



Art. 26,  
Art. 27,  
Art. 86



# Anbieterpflichten bezüglich der Anforderungen an Hochrisiko-KI-Systeme (Auswahl)

Risikomanagementsystem

Daten-Governance

Technische  
Dokumentation

Aufzeichnungspflichten

Aufzeichnungspflichten

Transparenzpflichten

Menschliche Aufsicht

Genauigkeit

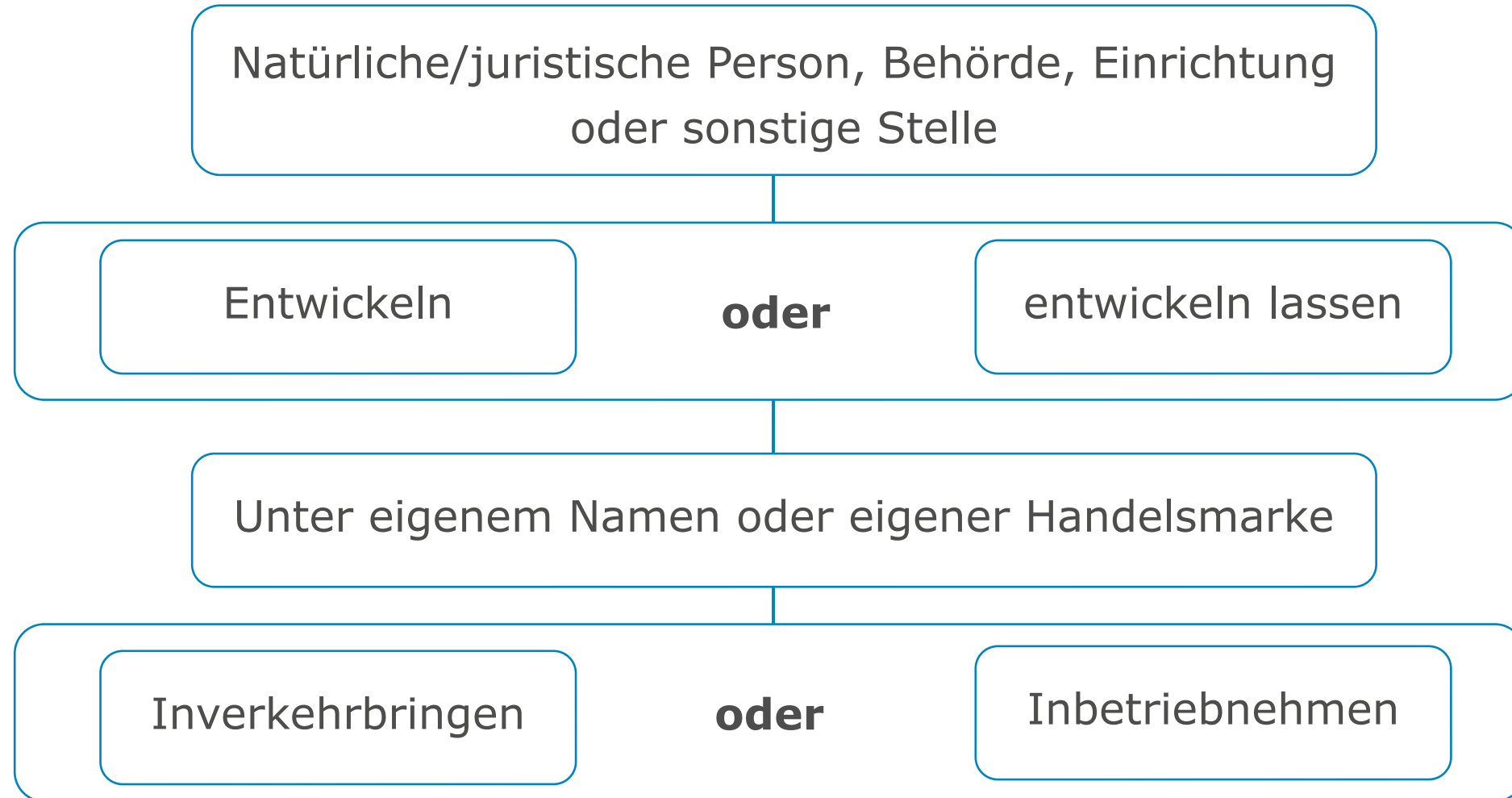
Robustheit

Cybersicherheit

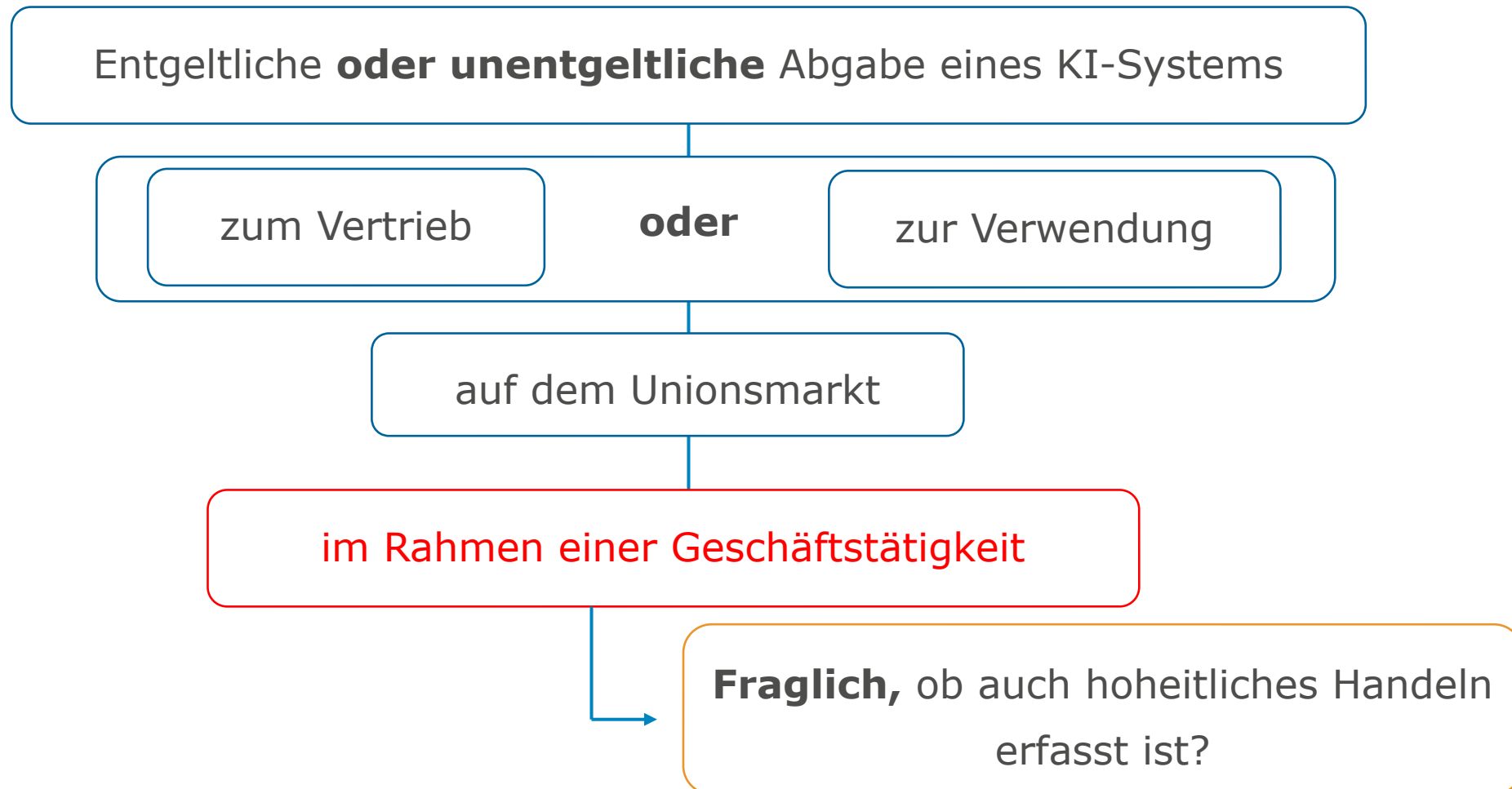
Qualitätsmanagement-  
system

Korrekturmaßnahmen

# Anbieterin (Art. 3 Nr. 3 KI-VO)

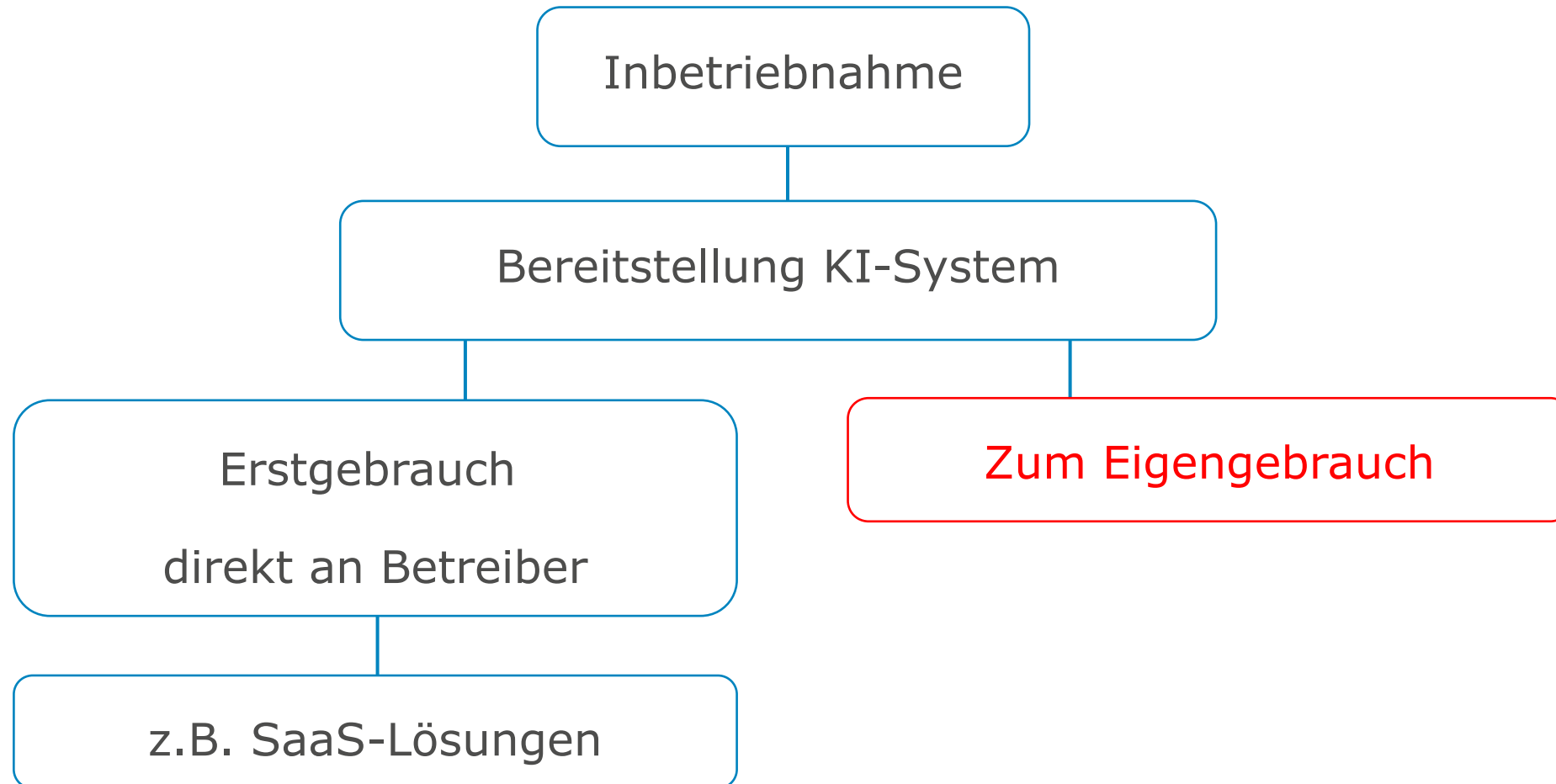


# Inverkehrbringen = Bereitstellung auf dem Markt

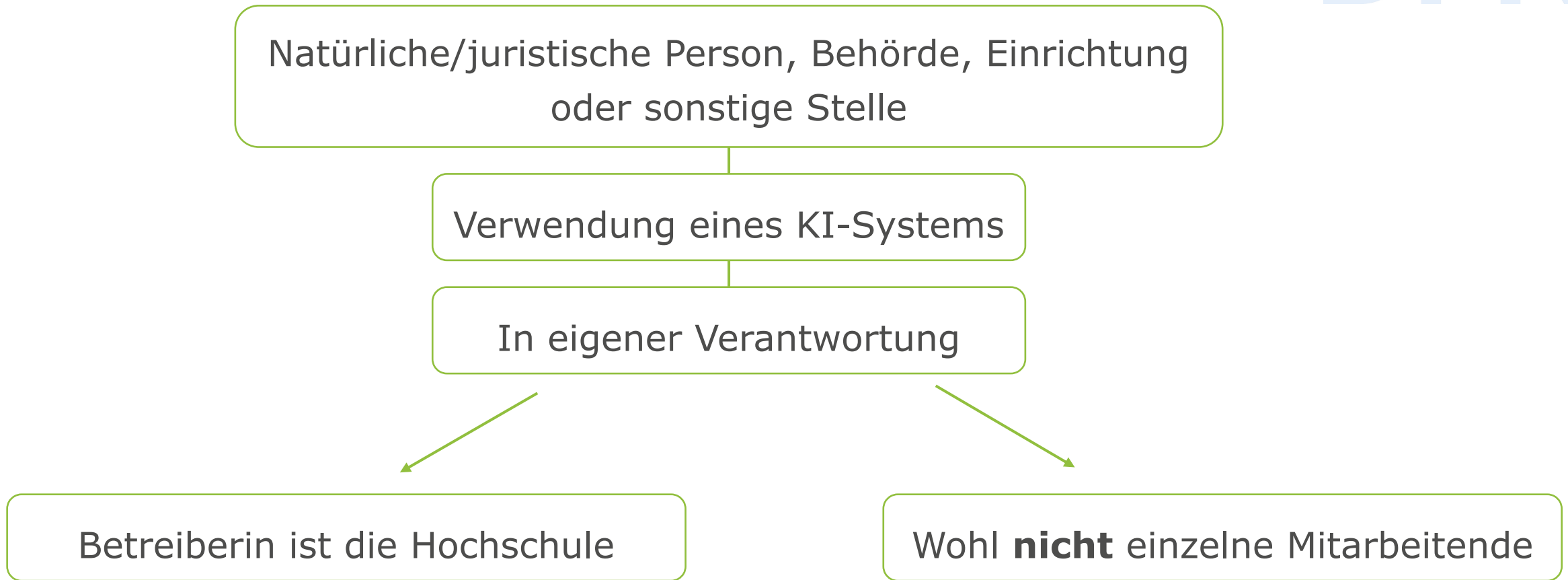




# Anbieterin (Art. 3 Nr. 3 KI-VO)

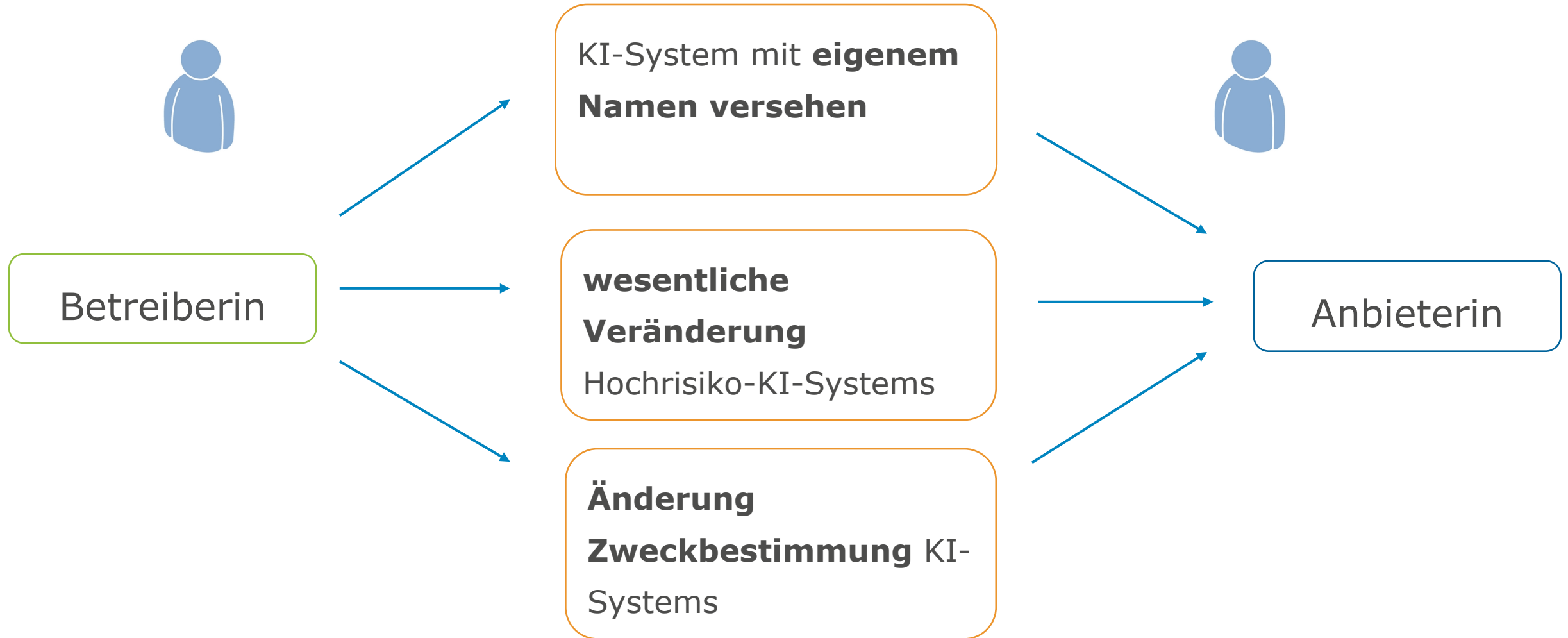


# Betreiberin (Art. 3 Nr. 4 KI-VO)



Ausnahme: persönliche und nicht berufliche Tätigkeit

# Betreiberin wird zur Quasi-Anbieterin (Art. 25 KI-VO)



# DFN

## Verbotene KI



# Verbotene KI-Systeme (Art. 5 KI-VO)

**Manipulation** (z.B. unterschwellige Beeinflussung)

**Emotionserkennung** am Arbeitsplatz oder in Bildungseinrichtungen (Ausnahme z.B. für Sicherheitsgründe)

**Biometrische Kategorisierung**

**Social Scoring**

**Gesichtsdatenbanken** (durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen)

# Exkurs: Social Scoring

**Bewertung**/Einstufung von  
Personen/Personengruppen



Über einen bestimmten  
Zeitraum



Auf Grundlage sozialen  
Verhaltens oder bekannter,  
abgeleiteter oder vorhergesagter  
persönlicher Eigenschaften oder  
Persönlichkeitsmerkmal

**Schlechterstellung**  
oder **Benachteiligung**

steht in **keinem**  
**Zusammenhang** zu den  
Umständen, unter denen die  
Daten ursprünglich erzeugt  
oder erhoben wurden

**oder**

im Hinblick auf soziales  
Verhalten oder dessen  
Tragweite **ungerechtfertigt**  
**oder unverhältnismäßig**

# DFN

## Hochrisiko-KI



## Produktbezogen

Produkt oder Sicherheitsbauteil eines Produkts nach Anhang I (z.B. Kinderspielzeug, Seilbahnen)



Produkt unterliegt einer Konformitätsbewertung durch Dritte

## Anwendungsbezogen

Biometrie

Kritische Infrastruktur

Bildung

Beschäftigung und Personalmanagement

Zugang zu grundlegenden Diensten und Leistungen

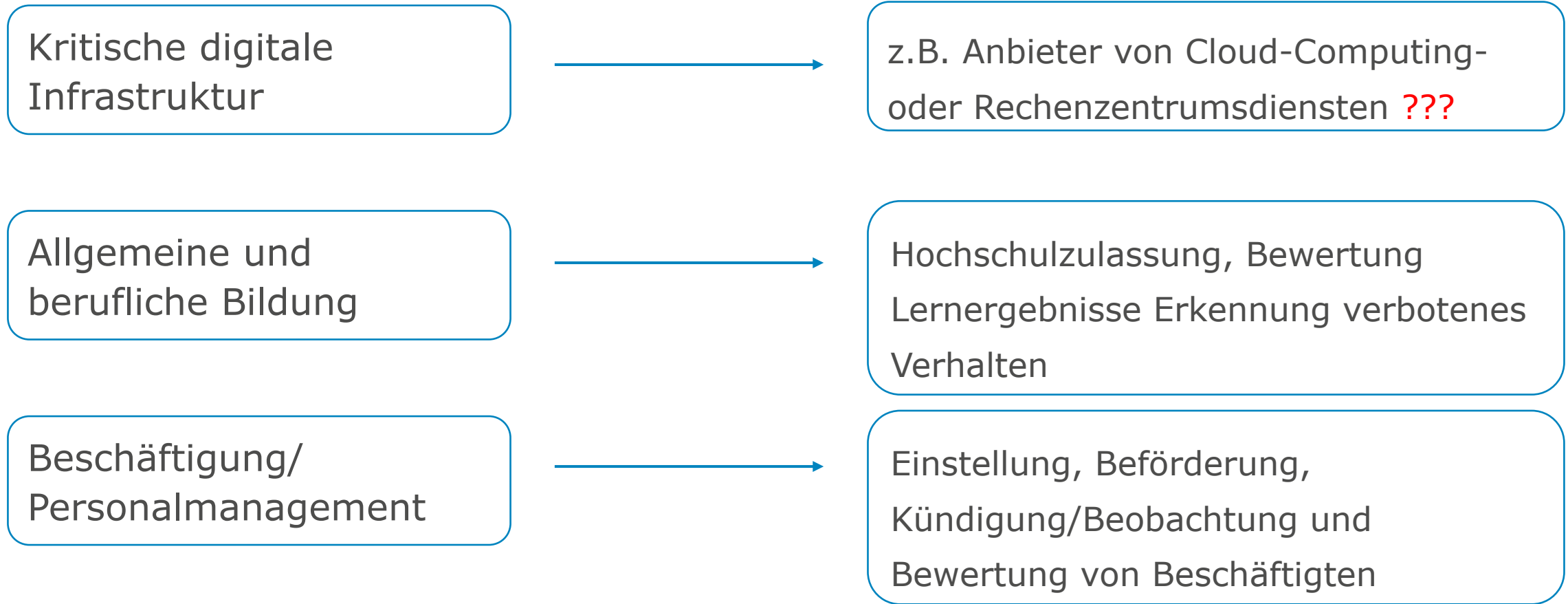
Strafverfolgung

Migration, Asyl und Grenzkontrolle

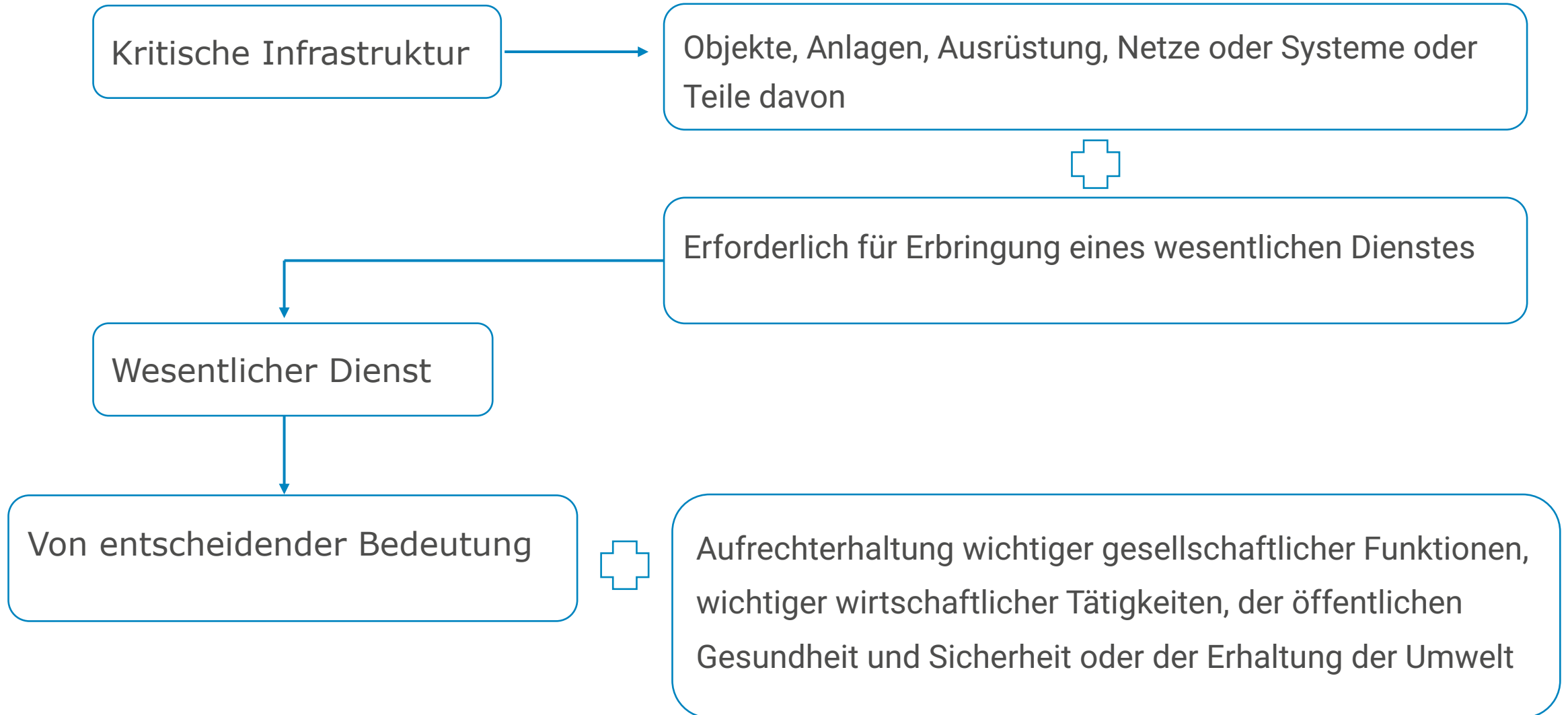
Rechtspflege und demokratische Prozesse



# Im Hochschulkontext relevante Anwendungsbereiche von Hochrisiko-KI-Systemen



# Kritische Infrastrukturen (Art. 3 Nr. 62 KI-VO)



# Mögliche kritische Einrichtungen

## NIS-2-RL

Betreiber Internet-Knoten

Anbieter Cloud-Computing-Dienste

DNS-Diensteanbieter

Betreiber Internet-Knoten

TLD-Namenregister

Anbieter Rechenzentrumsdienste

## eIDAS-VO

Vertrauensdienste-anbieter (Art. 3 Nr. 19)

## RL (EU)

**2018/1972**

Anbieter öffentlicher elektronischer Kommunikationsnetze

Anbieter elektron. Kommunikationsdienste, die öffentlich zugänglich sind

## **Immatrikulation**

**Zugang**, Zulassung oder zur Zuweisung natürlicher Personen zu Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung

**z.B. Klausuren-  
korrektur**

**Bewertung** von Lernergebnissen und des angemessenen Bildungsniveaus

**Plagiatssoftware**

?

**Überwachung** und Erkennung von verbotenen Verhalten bei Prüfungen

# Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

**Vor** dem  
Arbeitsverhältnis

**Einstellung** oder **Auswahl** natürlicher Personen (insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber:innen zu bewerten)

**Während** des  
Arbeitsverhältnisses

**Entscheidungen**, die Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen; **Zuweisung** von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften; oder **Beobachtung** und **Bewertung** von Leistungen oder Verhalten

# Ausnahmen (Einstufung durch Anbieterin)



# Überblick Pflichten Betreiberin von Hochrisiko-KI

## Vor Inbetriebnahme

Grundrechte-  
Folgenabschätzung

Information  
betroffener  
Arbeitnehmer:innen

## Beim Betrieb

Verwenden der Betriebsanleitung

Repräsentative Eingabedaten

Menschliche Aufsicht

Überwachung des Betriebs

Aufbewahrung der Protokolle

## Anlassbezogen

Recht auf Erklärung

Meldung schwerer Vorfälle

# Grundrechte-Folgenabschätzung (Art. 27 KI-VO)

## Voraussetzungen

Anwendungsbezogene  
Hochrisiko-KI

Einrichtungen öff. Rechts  
oder Private, die  
öffentliche Dienste  
erbringen

Ausnahme: kritische  
Infrastruktur

## Inhalt

1. Verfahren

4. spezifischen  
Schadensrisiken

2. Zeitraum und  
Häufigkeit

5. menschliche  
Aufsicht

3.  
Personenkategorien

6. Risikomaßnahmen



# Vergleich mit Datenschutz- Folgenabschätzung (Art. 35 DSGVO)

## KI-VO

1. Verfahren

4. spezifische  
Schadensrisiken

2. Zeitraum und  
Häufigkeit

5. menschliche  
Aufsicht

3.  
Personenkategorien

6.  
Risikomaßnahmen

## DSGVO

1. Verarbeitungs-  
vorgänge und  
Zwecke

3. spezifische  
Schadensrisiken

2. Notwendigkeit  
und  
Verhältnismäßigkeit

4. geplante  
Abhilfemaßnahmen

# Recht auf Erklärung

Art. 86 Abs. 1 KI-VO = Art. 15 Abs. 1 lit. h iVm Art. 22 Abs. 1 DSGVO

Person ist von einer  
Entscheidung  
betroffen

Entscheidung beruht  
auf Hochrisiko-KI-  
System

Ausnahme für  
kritische Infrastruktur

rechtliche Auswirkung  
oder beeinträchtigt  
Grundrechte



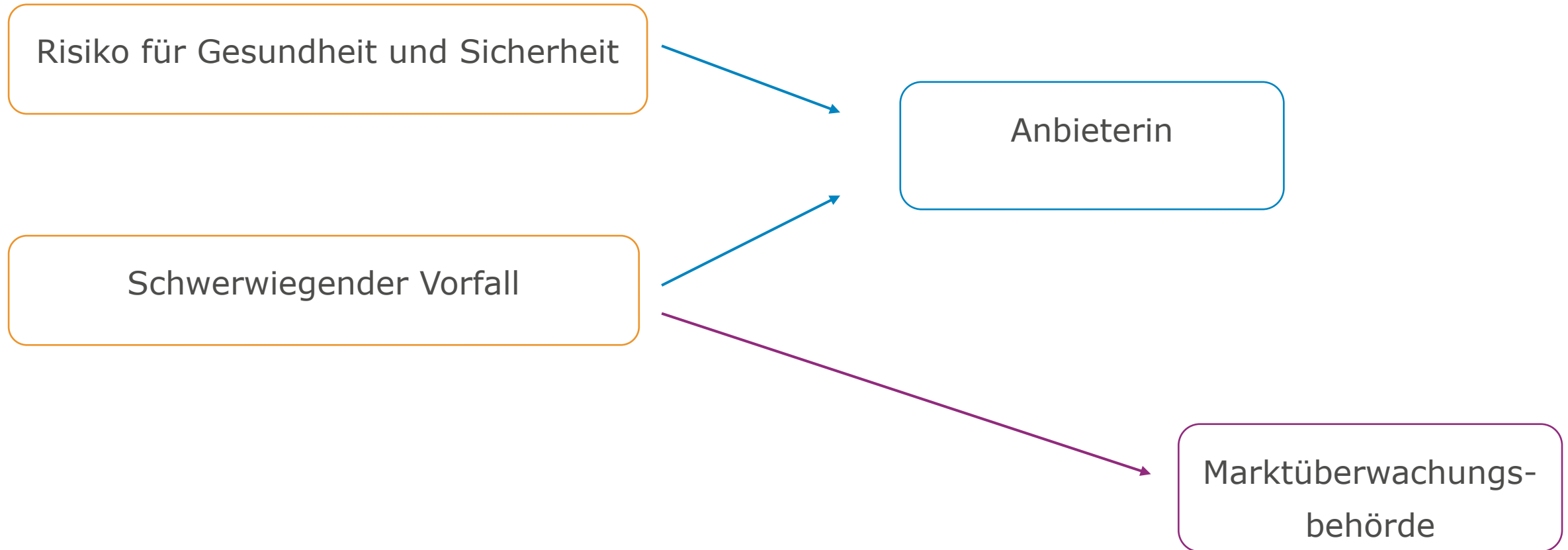
klare und aussagekräftige Erläuterung

zur Rolle des KI-Systems im  
Entscheidungsprozess



zu den wichtigsten Elementen der  
getroffenen Entscheidung

# Informationspflichten der Betreiberin



Schwerwiegender Vorfall



1. Tod oder schwere gesundheitliche Schädigung einer Person
2. schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen
3. Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte
4. schwere Sach- oder Umweltschäden

# DFN

Beschränktes Risiko



# Beschränktes Risiko: Transparenzanforderungen

## Anwendungen

Emotionserkennung oder  
biometrische Kategorisierung

Erstellung von Deepfakes

## Pflichten

Information der betroffenen  
Person

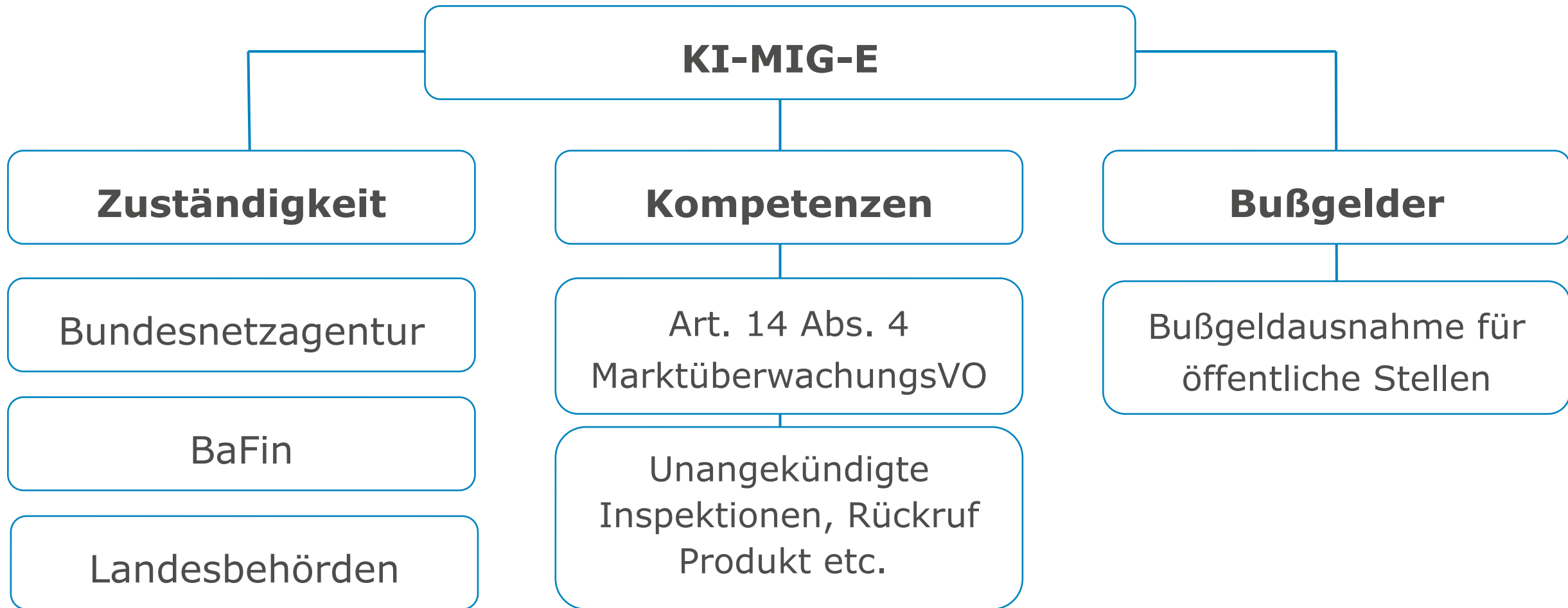
Kenntlichmachung

Es sei denn, es ist  
offensichtlich

DFN

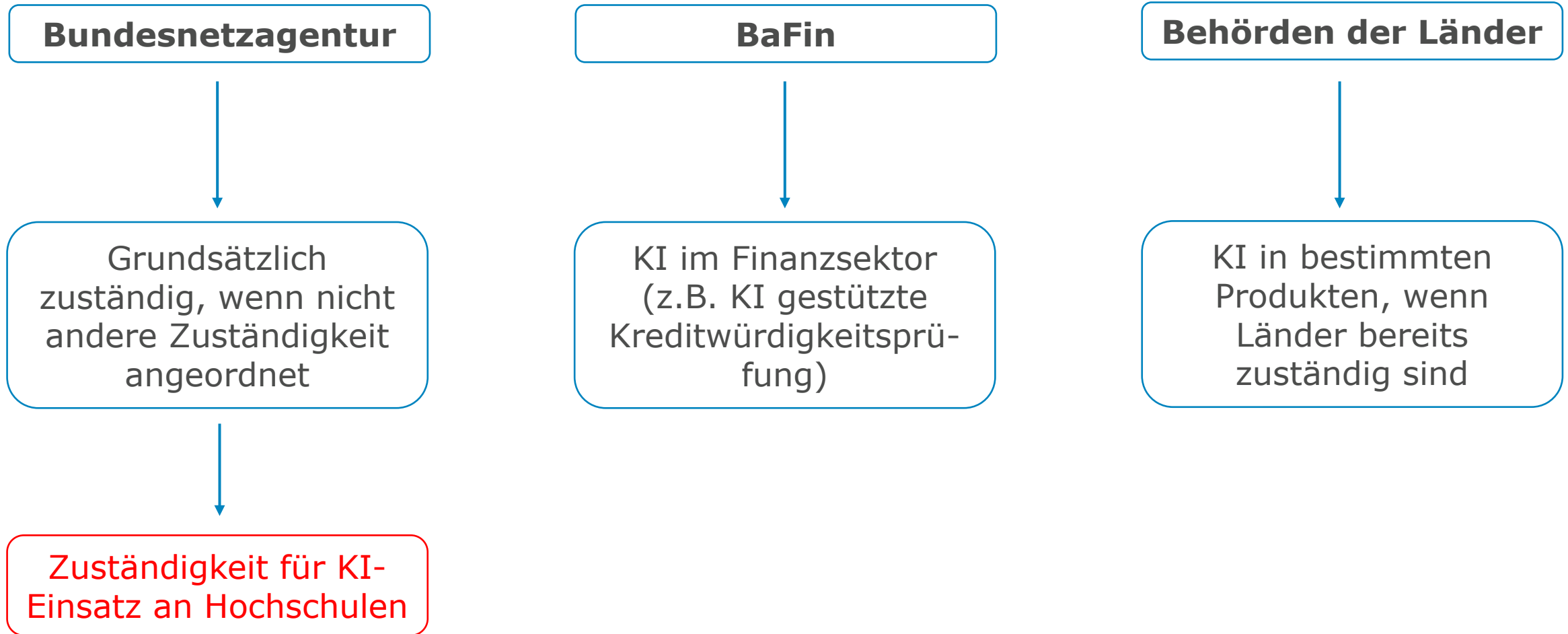
## KI-Aufsicht in Deutschland







# Zuständigkeit für die Einhaltung der KI-VO



# Bußgeldvorschriften (§ 15 KIMIG-E)

Bußgelder für Betreiber von Hochrisiko-KI-Systemen: **bis zu** 15 Mio. oder 3% gesamter weltweiter Jahresumsatz (Art. 99 Abs. 3 KI-VO iVm § 15 Abs. 1 KIMIG-E)

→ **Ausnahme** für öffentliche Stellen nach § 15 Abs. 4 KIMIG-E iVm § 2 Abs. 1, 2 BDSG (gilt auch für staatliche Hochschulen)

→ Gilt nicht für Beliehene, weil kein Verweis auf § 2 Abs. 4 S. 2 BDSG  
= keine Bußgeldausnahme für private Hochschulen

# Mögliche Europarechtswidrigkeit von § 15 Abs. 4 KIMIG-E

Kompetenz zur Regelung von Bußgeldern gegenüber öffentlichen Stellen (Art. 99 Abs. 8 KI-VO)

„in welchem Umfang“: fraglich ob auch Bußgeldausschluss

Vergleich zu Art. 83 Abs. 7 DSGVO: „**ob** und in welchem Umfang“

# Haben Sie noch Fragen?



## ► Kontakt

### ► Forschungsstelle Recht im DFN

E-Mail: [recht@dfn.de](mailto:recht@dfn.de)

Telefon: 030 2093-91443

Anschrift:

Forschungsstelle Recht im DFN  
Humboldt-Universität zu Berlin

Unter den Linden 11

10117 Berlin

### ► Philipp Schöbel

E-Mail: [philipp.manuel.schoebel@hu-berlin.de](mailto:philipp.manuel.schoebel@hu-berlin.de)

Telefon: 030 2093-91443

Anschrift:

Forschungsstelle Recht im DFN  
Humboldt-Universität zu Berlin

Unter den Linden 11

10117 Berlin

