deutsches forschungsnetz

Der AI Act und die Wissenschaftsfreiheit

DFN-Betriebstagung | 25.03.2025

Philipp Schöbel

Gliederung

1. Konzeption des AI Acts
    1. Begriffe
    2. Akteure
    3. Ausnahmen
2. Verbotene KI
3. KI mit beschränktem Risiko
4. Hochrisiko-KI
    1. Klassifizierung
    2. Pflichten

Konzeption des AI Acts

Konzeption des AI Acts (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?

„ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“

(Art. 3 Nr. 1 AI Act)

Was ist ein KI-System?

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

Was ist ein KI-System?

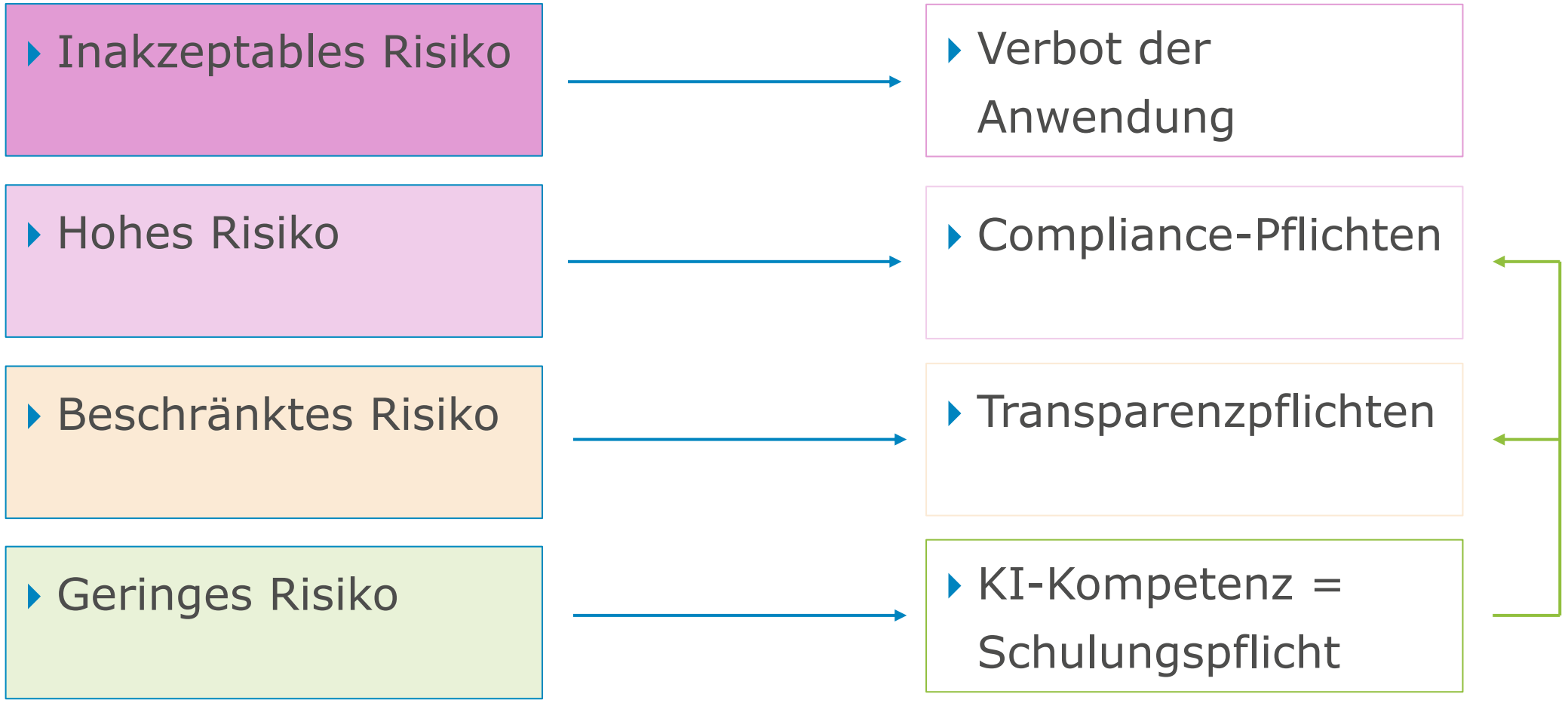
- autonomer Betrieb

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 ausschließlich von natürlichen Personen definierte Regeln für das automatische Ausführen von Operationen.

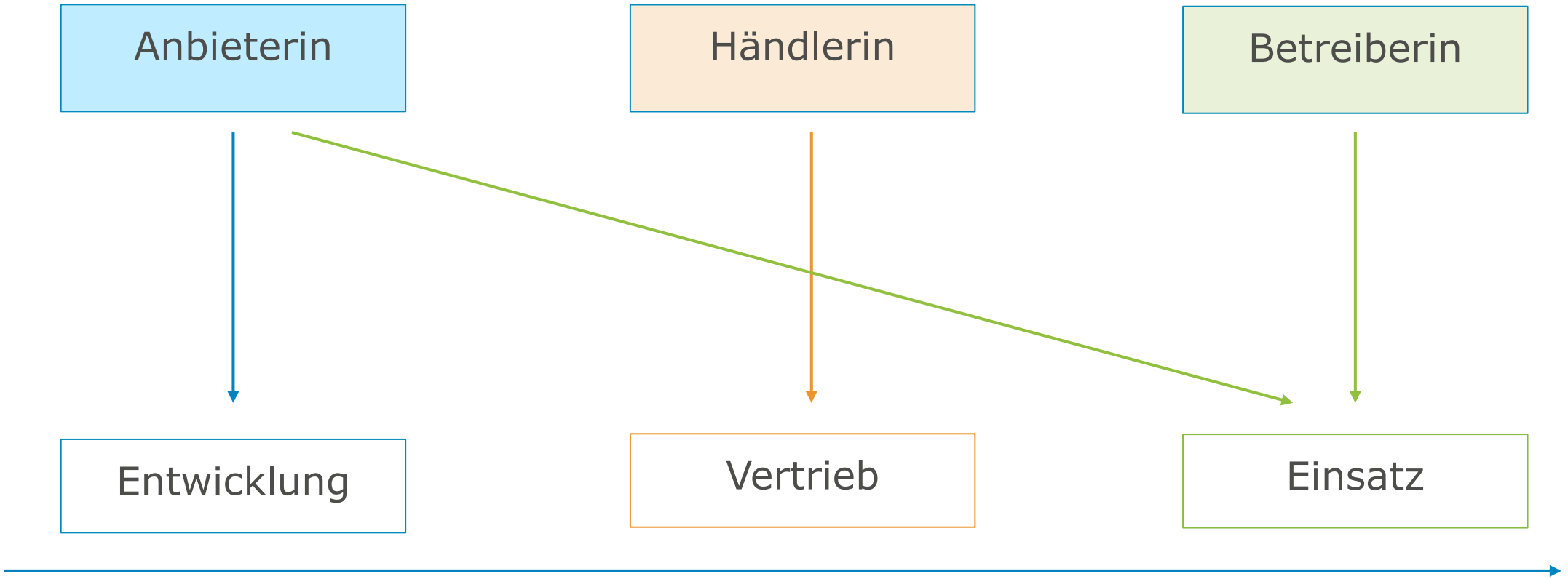
- Ableiten

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.

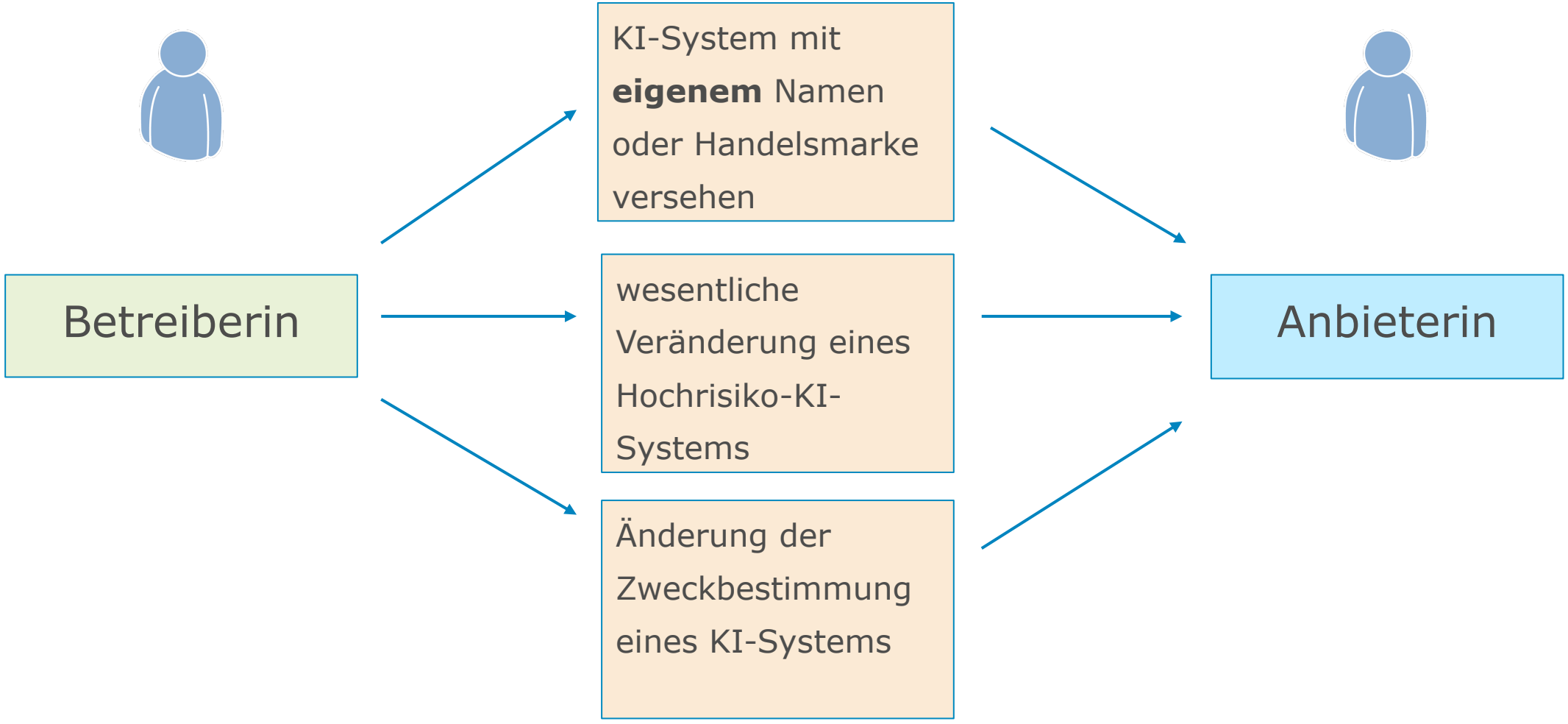
Risikogruppen für KI-Systeme



Akteure des AI Acts



Betreiberin wird zur Anbieterin



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

Ausnahmen für die Wissenschaft

Forschung **an** KI (Art. 2 Abs. 8 AI Act)

AI Act gilt nicht für für Forschungs-, Test- und Entwicklungstätigkeiten zu KI

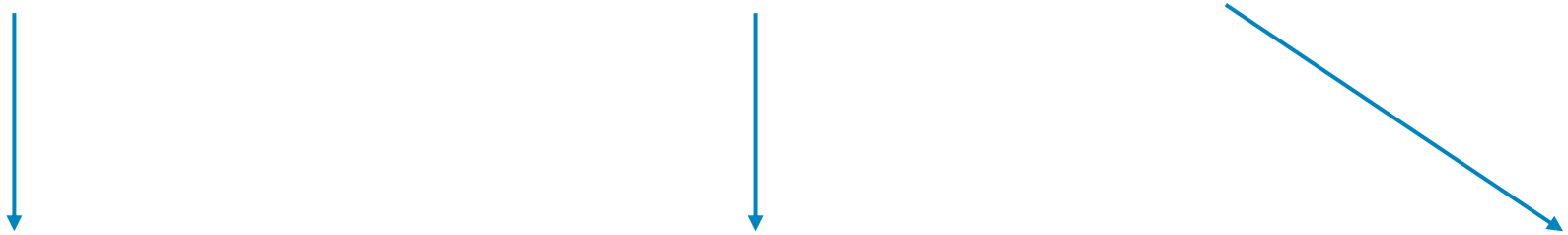
Ausnahme: Tests unter Realbedingungen

Forschung **mit** KI (Art. 2 Abs. 6 AI Act)

AI Act gilt nicht für KI, die ausschließlich für Forschung in Betrieb genommen wird

Ausnahmen für die Wissenschaft

- AI Act 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 AI Act).



- AI Act gilt für Verwaltungstätigkeiten an Hochschulen
- AI Act gilt für Lehrtätigkeiten an Hochschulen
- Ausnahme gilt nicht für dual-use (z.B. Forschung und Lehre)

KI-Kompetenz

- Fähigkeiten
- Kenntnisse
- Verständnis

- Sachkundiger Einsatz
- Bewusstsein für Chancen und Risiken

Verbotene KI

Verbotene KI-Systeme

Artikel 5[1] Verbotene Praktiken im KI-Bereich

(1) 1Folgende Praktiken im KI-Bereich sind verboten:

a)das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird.

b)das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung ausnutzt, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird;

c)das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt:

i)Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden;

ii)Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in einer Weise, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist;

d)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen; dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen;

e)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern;

f)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen, es sei denn, die Verwendung des KI-Systems soll aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht werden;

g)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von Systemen zur biometrischen Kategorisierung, mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten kategorisiert werden, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten; dieses Verbot gilt nicht für die Kennzeichnung oder Filterung rechtmäßig erworbener biometrischer Datensätze, wie z.B. Bilder auf der Grundlage biometrischer Daten oder die Kategorisierung biometrischer Daten im Bereich der Strafverfolgung;

h)die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:

i)gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;

ii)Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags;

iii)Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in Anhang II aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist.

Verbotene KI-Systeme

2Unterabsatz 1 Buchstabe h gilt unbeschadet des Artikels 9 der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung.

(2) 1Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele darf für die in jenem Buchstaben genannten Zwecke nur zur Bestätigung der Identität der speziell betroffenen Person erfolgen, wobei folgende Elemente berücksichtigt werden:

a)die Art der Situation, die der möglichen Verwendung zugrunde liegt, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß des Schadens, der entstehen würde, wenn das System nicht eingesetzt würde;

b)die Folgen der Verwendung des Systems für die Rechte und Freiheiten aller betroffenen Personen, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß solcher Folgen.

2Darüber hinaus sind bei der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h des vorliegenden Artikels genannten Ziele notwendige und verhältnismäßige Schutzvorkehrungen und Bedingungen für die Verwendung im Einklang mit nationalem Recht über die Ermächtigung ihrer Verwendung einzuhalten, insbesondere in Bezug auf die zeitlichen, geografischen und personenbezogenen Beschränkungen. 3Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen ist nur dann zu gestatten, wenn die Strafverfolgungsbehörde eine Folgenabschätzung im Hinblick auf die Grundrechte gemäß Artikel 27 abgeschlossen und das System gemäß Artikel 49 in der EU-Datenbank registriert hat. 4In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung solcher Systeme zunächst ohne Registrierung in der EU-Datenbank begonnen werden, sofern diese Registrierung unverzüglich erfolgt.

(3)[1] 1Für die Zwecke des Absatz 1 Unterabsatz 1 Buchstabe h und des Absatzes 2 ist für jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eine vorherige Genehmigung erforderlich, die von einer Justizbehörde oder einer unabhängigen Verwaltungsbehörde des Mitgliedstaats, in dem die Verwendung erfolgen soll, auf begründeten Antrag und gemäß den in Absatz 5 genannten detaillierten nationalen Rechtsvorschriften erteilt wird, wobei deren Entscheidung bindend ist. 2In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung eines solchen Systems zunächst ohne Genehmigung begonnen werden, sofern eine solche Genehmigung unverzüglich, spätestens jedoch innerhalb von 24 Stunden beantragt wird. 3Wird eine solche Genehmigung abgelehnt, so wird die Verwendung mit sofortiger Wirkung eingestellt und werden alle Daten sowie die Ergebnisse und Ausgaben dieser Verwendung unverzüglich verworfen und gelöscht.

[2] 1Die zuständige Justizbehörde oder eine unabhängige Verwaltungsbehörde, deren Entscheidung bindend ist, erteilt die Genehmigung nur dann, wenn sie auf der Grundlage objektiver Nachweise oder eindeutiger Hinweise, die ihr vorgelegt werden, davon überzeugt ist, dass die Verwendung des betreffenden biometrischen Echtzeit-Fernidentifizierungssystems für das Erreichen eines der in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele – wie im Antrag angegeben – notwendig und verhältnismäßig ist und insbesondere auf das in Bezug auf den Zeitraum sowie den geografischen und persönlichen Anwendungsbereich unbedingt erforderliche Maß beschränkt bleibt. 2Bei ihrer Entscheidung über den Antrag berücksichtigt diese Behörde die in Absatz 2 genannten Elemente. 3Eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, darf nicht ausschließlich auf der Grundlage der Ausgabe des biometrischen Echtzeit-Fernidentifizierungssystems getroffen werden.

(4) 1Unbeschadet des Absatzes 3 wird jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken der zuständigen Marktüberwachungsbehörde und der nationalen Datenschutzbehörde gemäß den in Absatz 5 genannten nationalen Vorschriften mitgeteilt. 2Die Mitteilung muss mindestens die in Absatz 6 genannten Angaben enthalten und darf keine sensiblen operativen Daten enthalten.

(5) 1Ein Mitgliedstaat kann die Möglichkeit einer vollständigen oder teilweisen Ermächtigung zur Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken innerhalb der in Absatz 1 Unterabsatz 1 Buchstabe h sowie Absätze 2 und 3 aufgeführten Grenzen und unter den dort genannten Bedingungen vorsehen. 2Die betreffenden Mitgliedstaaten legen in ihrem nationalen Recht die erforderlichen detaillierten Vorschriften für die Beantragung, Erteilung und Ausübung der in Absatz 3 genannten Genehmigungen sowie für die entsprechende Beaufsichtigung und Berichterstattung fest. 3In diesen Vorschriften wird auch festgelegt, im Hinblick auf welche der in Absatz 1 Unterabsatz 1 Buchstabe h aufgeführten Ziele und welche der unter Buchstabe h Ziffer iii genannten Straftaten die zuständigen Behörden ermächtigt werden können, diese Systeme zu Strafverfolgungszwecken zu verwenden. 4Die Mitgliedstaaten teilen der Kommission diese Vorschriften spätestens 30 Tage nach ihrem Erlass mit. 5Die Mitgliedstaaten können im Einklang mit dem Unionsrecht strengere Rechtsvorschriften für die Verwendung biometrischer Fernidentifizierungssysteme erlassen.

(6) 1Die nationalen Marktüberwachungsbehörden und die nationalen Datenschutzbehörden der Mitgliedstaaten, denen gemäß Absatz 4 die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken mitgeteilt wurden, legen der Kommission Jahresberichte über diese Verwendung vor. 2Zu diesem Zweck stellt die Kommission den Mitgliedstaaten und den nationalen Marktüberwachungs- und Datenschutzbehörden ein Muster zur Verfügung, das Angaben über die Anzahl der Entscheidungen der zuständigen Justizbehörden oder einer unabhängigen Verwaltungsbehörde, deren Entscheidung über Genehmigungsanträge gemäß Absatz 3 bindend ist, und deren Ergebnis enthält.

(7) 1Die Kommission veröffentlicht Jahresberichte über die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, die auf aggregierten Daten aus den Mitgliedstaaten auf der Grundlage der in Absatz 6 genannten Jahresberichte beruhen. 2Diese Jahresberichte dürfen keine sensiblen operativen Daten im Zusammenhang mit den damit verbundenen Strafverfolgungsmaßnahmen enthalten.

(8) Dieser Artikel berührt nicht die Verbote, die gelten, wenn KI-Praktiken gegen andere Rechtsvorschriften der Union verstoßen.

Verbotene KI-Systeme

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

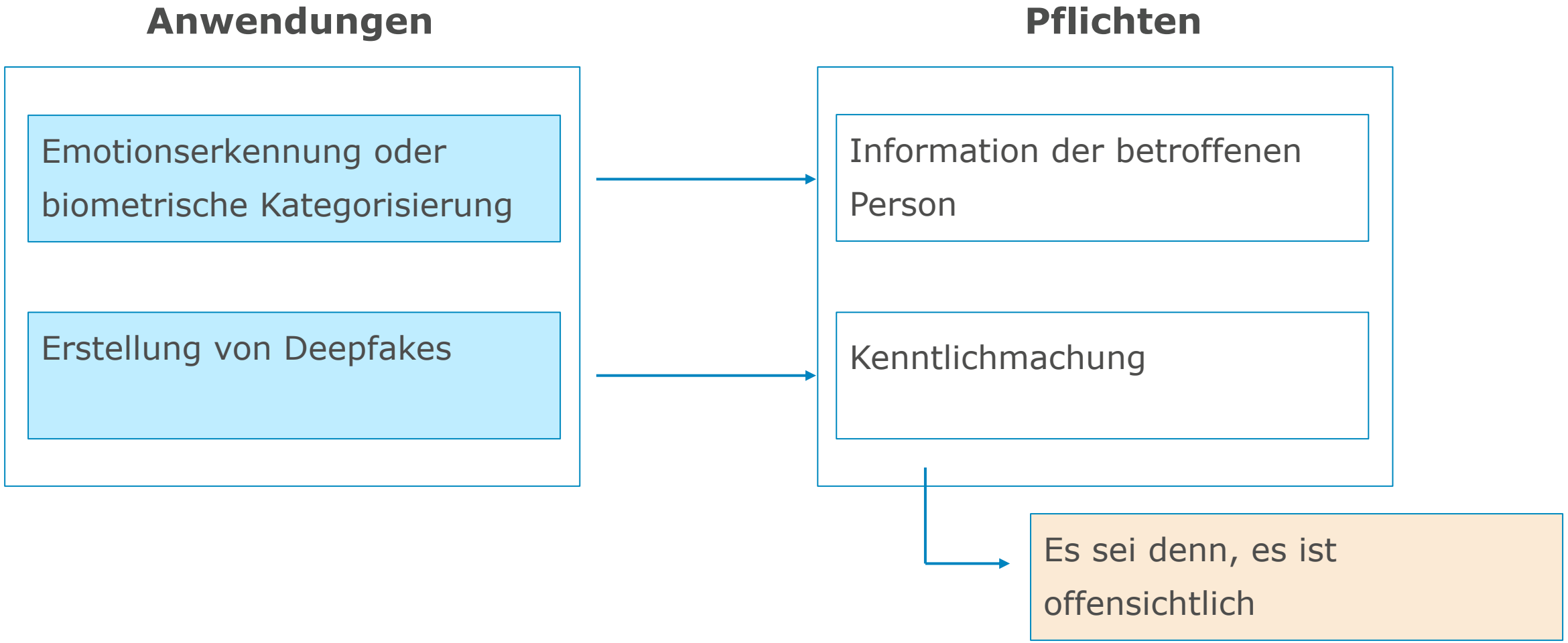
oder

im Hinblick auf soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig

DFN

Beschränktes Risiko

Beschränktes Risiko: Transparenzanforderungen



DFN

Hochrisiko-KI

Klassifizierung von Hochrisiko-KI-Systemen

Produktbezogen

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

✚

Produkt unterliegt einer Konformitätsbewertung durch Dritte

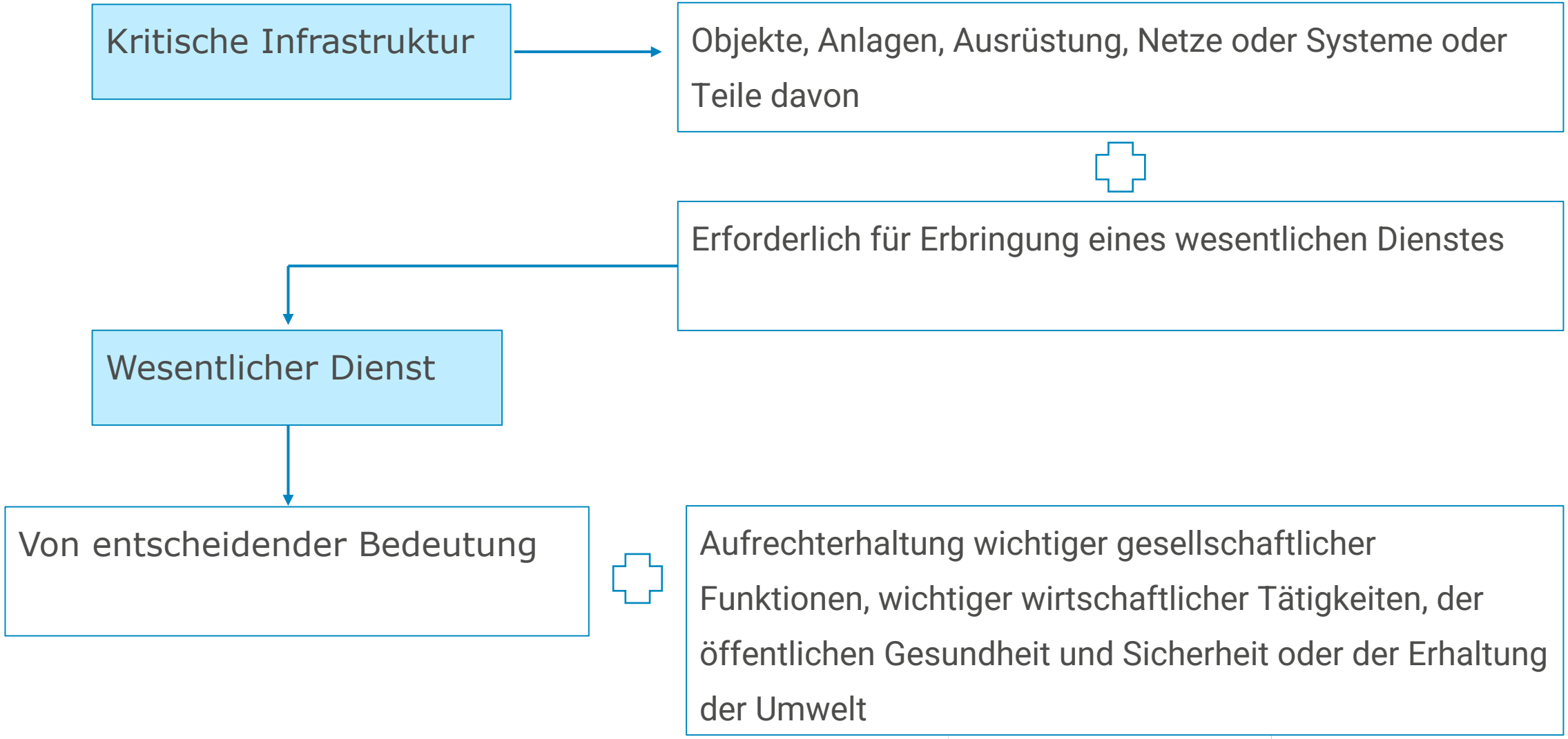
Anwendungsbezogen

- Biometrie
- Kritische Infrastruktur
- Bildung
- Beschäftigung u. 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 digitale Infrastruktur	z.B. Anbieter von Cloud-Computing- oder Rechenzentrumsdiensten ???
Allgemeine und berufliche Bildung	Hochschulzulassung, Bewertung Lernergebnissen und Erkennung von verbotenem Verhalten
Beschäftigung/Personal management	Einstellung, Beförderung und Kündigung/Beobachtung und Bewertung von Beschäftigten

Kritische Infrastrukturen (Art. 3 Nr. 62 AI Act)



Mögliche kritische Einrichtungen

NIS-2 RL

- Betreiber Internet-Knoten (Art. 6 Nr. 18)
- Anbieter Cloud-Computing-Dienste (Art. 6 Nr. 18)
- DNS-Diensteanbieter (Art. 6 Nr. 20)
- Betreiber Internet-Knoten (Art. 6 Nr. 30)
- TLD-Namenregister (Art. 6 Nr. 21)
- Anbieter Rechenzentrumsdienste (Art. 6 Nr. 31)

VO (EU) 910/2014

- Vertrauensdienste-anbieter (Art. 3 Nr. 19)

RL (EU) 2018/1972

- Anbieter öffentlicher elektronischer Kommunikationsnetze (Art. 2 Nr. 8)
- Anbieter elektro. Kommd., öffentlich zugänglich sind (Art. 2 Nr. 4)

Allgemeine und berufliche Bildung

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 verbotenem 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 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)

kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte

(indem KI unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst)

- Durchführung eng gefasster Verfahrensaufgabe
- Verbesserung des Ergebnisses einer zuvor abgeschlossenen menschlichen Tätigkeit
- Erkennen von Entscheidungsmus-tern (kein Ersetzen menschlicher Bewertung)
- vorbereitende Aufgabe für eine Bewertung

Rückausnahme: Profiling

Definition: Art. 4 Nr. 4 DSGVO (Art. 3 Nr. 52)

Überblick Pflichten Betreiberin von Hochrisiko-KI

Vor Inbetriebnahme	Beim Betrieb	Anlassbezogen
Grundrechte-Folgenabschätzung	Verwenden der Betriebsanleitung	Recht auf Erklärung
Information betroffener Arbeitnehmer:innen	Repräsentative Eingabedaten	Meldung schwerer Vorfälle
	Menschliche Aufsicht	
	Überwachung des Betriebs	
	Aufbewahrung der Protokolle	

Grundrechte-Folgenabschätzung (Art. 27)

Voraussetzungen

- Anwendungsbezogene Hochrisiko-KI
- Einrichtungen öff. Rechts oder Private, die öffentliche Dienste erbringen
- Ausnahme: kritische Infrastruktur

Inhalt

1. Verfahren
2. Zeitraum und Häufigkeit
3. Personenkategorien
4. spezifischen Schadensrisiken
5. menschliche Aufsicht
6. Risikomaßnahmen

Vergleich mit Datenschutz-Folgenabschätzung(Art. 35 DSGVO)

AI Act

1. Verfahren
2. Zeitraum und Häufigkeit
3. Personenkategorien
4. spezifische Schadensrisiken
5. menschliche Aufsicht
6. Risikomaßnahmen

DSGVO

1. Verarbeitungs-vorgänge und Zwecke
2. Notwendigkeit und Verhältnismäßigkeit
3. spezifische Schadensrisiken
4. geplante Abhilfemaßnahmen

Recht auf Erklärung

Art. 86 Abs. 1 AI Act = 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

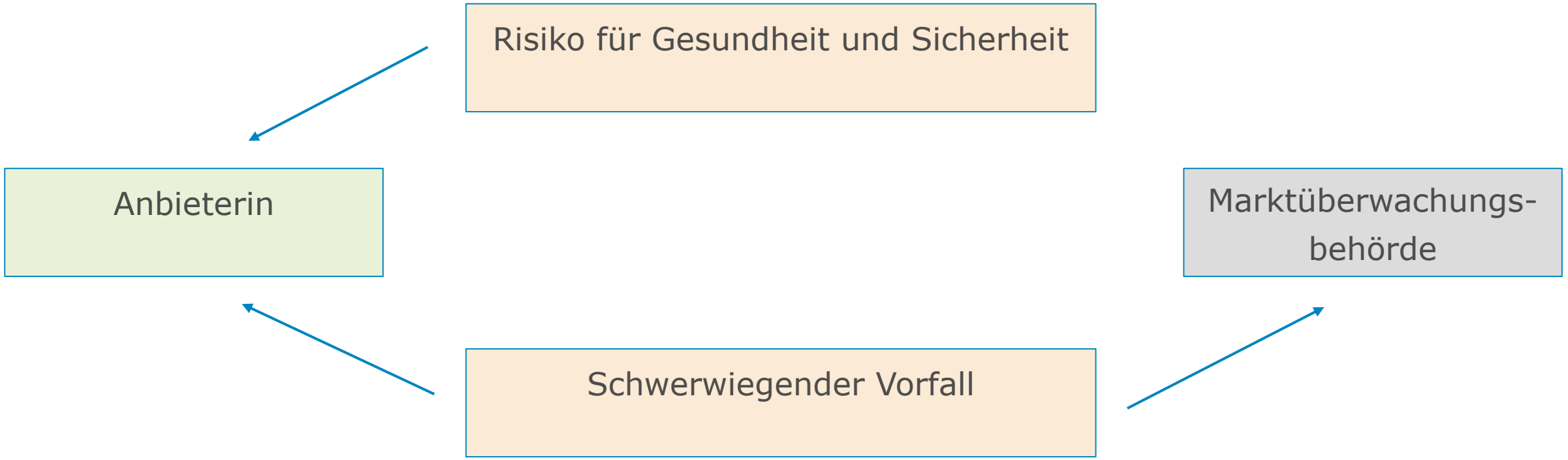
klare und aussagekräftige Erläuterung

zur Rolle des KI-Systems im Entscheidungsprozess

+

zu den wichtigsten Elementen der getroffenen Entscheidung

Informationspflichten der Betreiberin



Informationspflichten der Betreiberin

Risiko für Gesundheit und Sicherheit

Anbieterin

Marktüberwachungs-behörde

Schwerwiegender Vorfall

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

Haben Sie noch Fragen?

- Kontakt
  - Forschungsstelle Recht im DFN

    E-Mail: recht@dfn.de

    Telefon: 0251 83 – 38616/ 030 38 - 66754

    Anschrift:
    Forschungsstelle Recht im DFN
    Freie Universität Berlin
    Van't-Hoff-Straße 8
    14195 Berlin
  - Philipp Schöbel

    E-Mail: philipp.schoebel@fu-berlin.de

    Telefon: 030 38 - 66754

    Anschrift:
    Forschungsstelle Recht im DFN
    Freie Universität Berlin
    Van't-Hoff-Straße 8
    14195 Berlin