

# KI entlang der Lieferkette

Risiken beim Sourcing von KI und Einsatz entlang der Lieferkette

Digital Talks, 06.03.2024

RAin Marieke Luise Merkle

RAin Dr. Jasmin Schulzweida

# Live-Webinar: Hinweise



## Fragen

- Sie haben die Möglichkeit, live **über den Chat** Fragen zu stellen
- Wenn Sie eine Frage stellen, bleiben Sie gegenüber den übrigen Webinar-Teilnehmern **anonym**. Nur die Speaker sehen die von Ihnen gestellten Fragen
- Bitte haben Sie Verständnis dafür, dass wir ggf. nicht jede Frage beantworten können. Sie können gerne **im Nachgang** auf uns zukommen



## Präsentation

- Die Präsentation wird den Teilnehmern des Webinars **im Nachgang** zur Verfügung gestellt



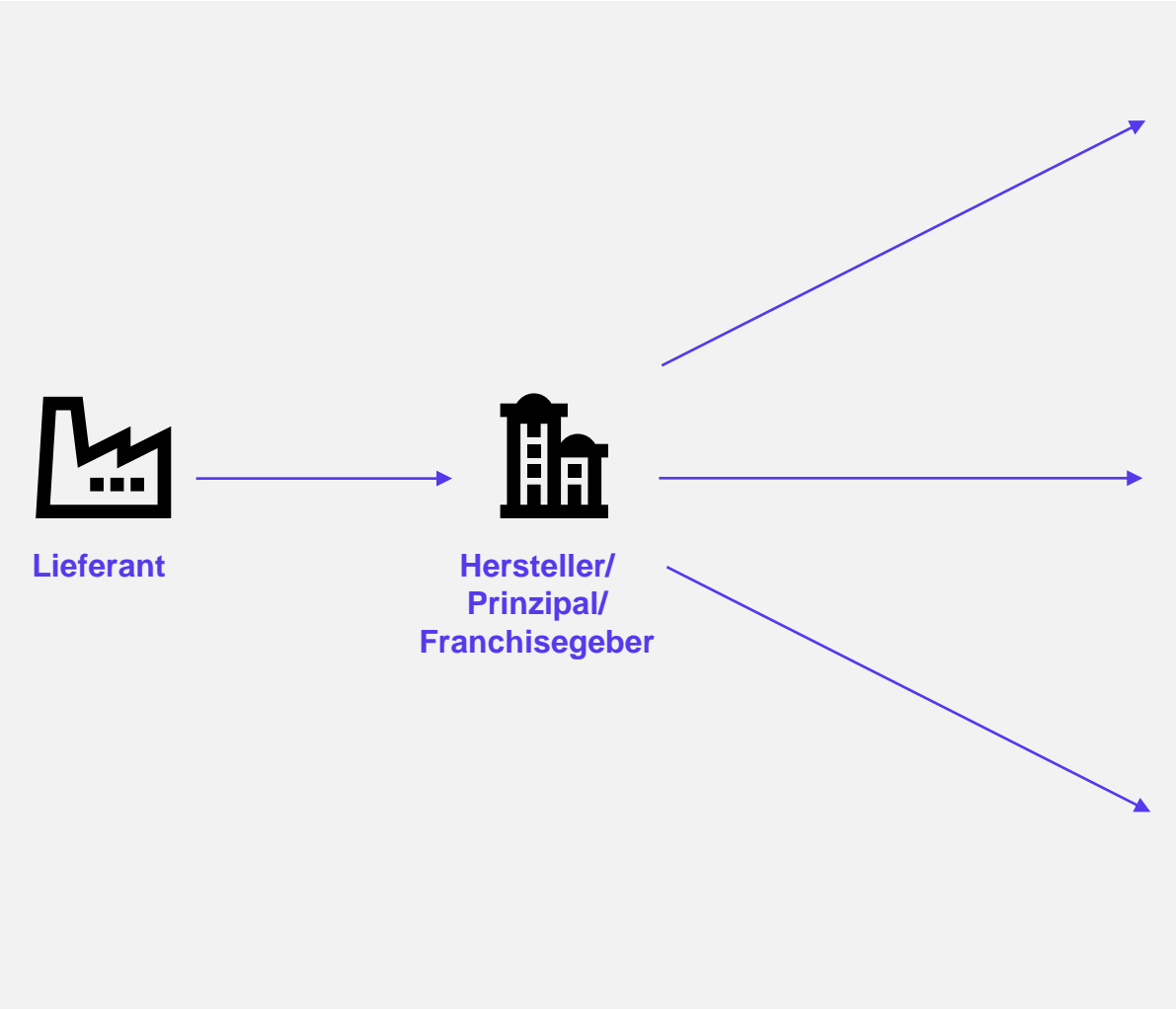
## Datenschutz

- Bitte beachten Sie, dass der Veranstalter **Video- und Audioaufzeichnungen** des Webinars machen kann und diese ggf. im Internet verbreitet

# Übersicht

- 1 Einführung
- 2 Risiken beim Sourcing von KI entlang der Lieferkette
- 3 Risiken beim Einsatz von KI entlang der Lieferkette
- 4 Fazit

# Einführung: Einsatz von KI entlang der Lieferkette



**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Vertragshändler**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung)

**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)

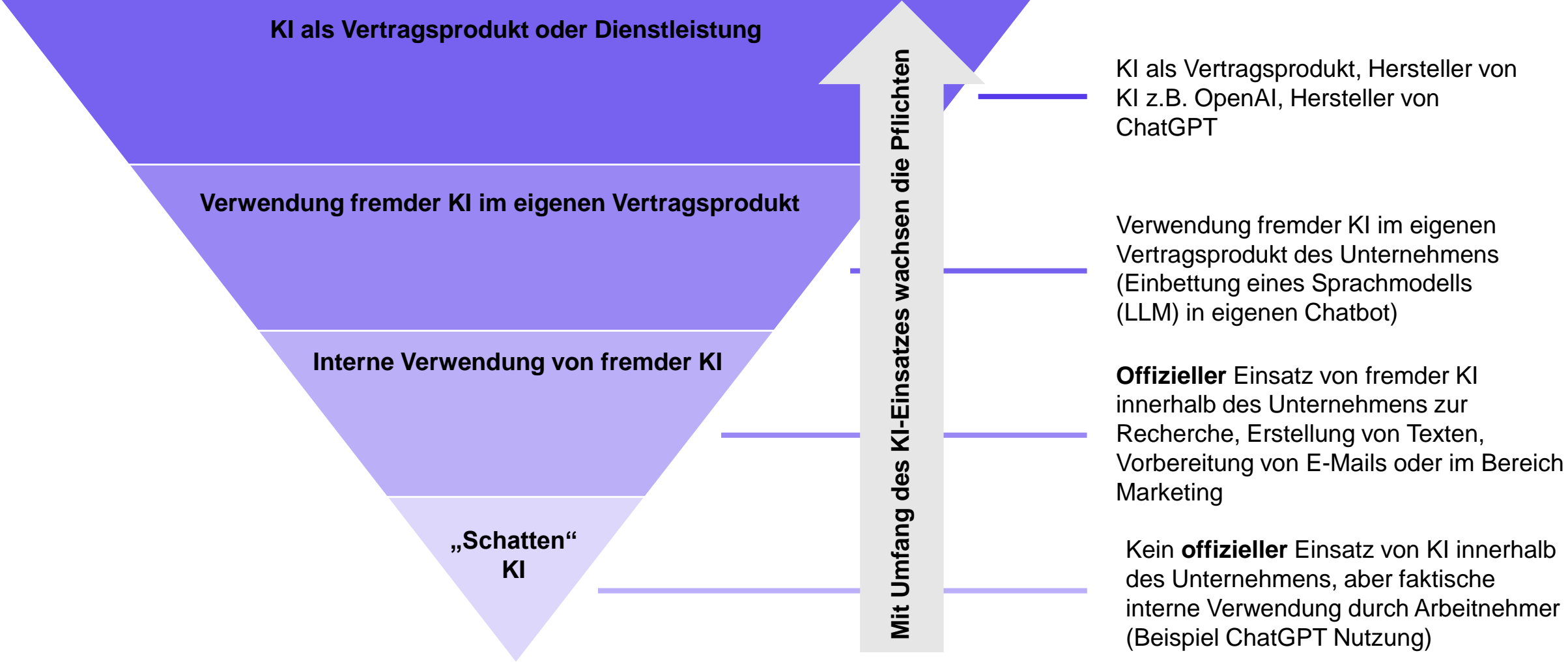
**1**

**KI Sourcing: KI als Gegenstand Vertragsprodukten oder Dienstleistungen**

**2**

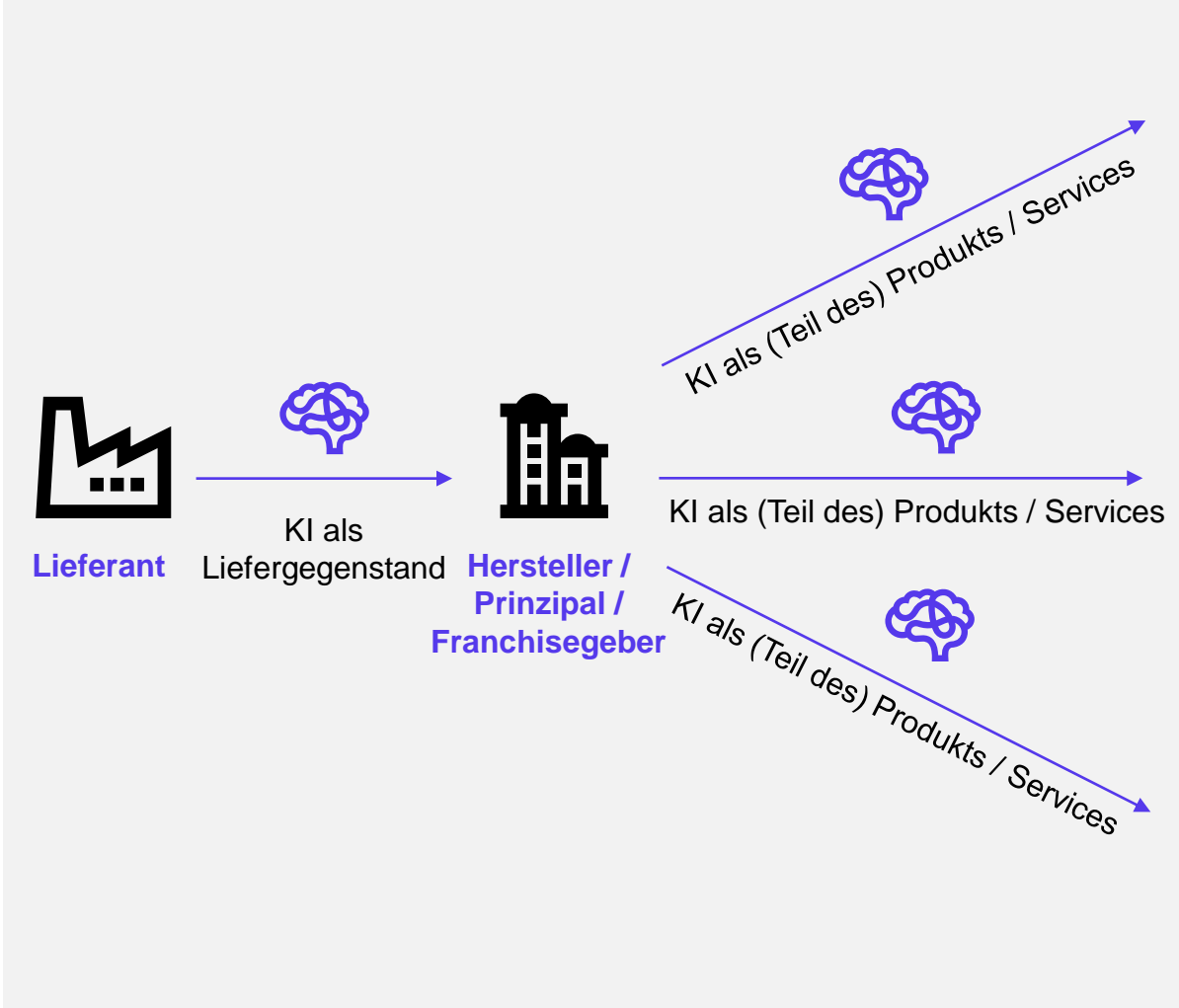
**Einsatz von KI durch „Player“ der Lieferkette**

# Einführung: Einsatz von KI entlang der Lieferkette



# Risiken beim Sourcing von KI

# KI entlang der Lieferkette – KI als Gegenstand von Produkten / Services

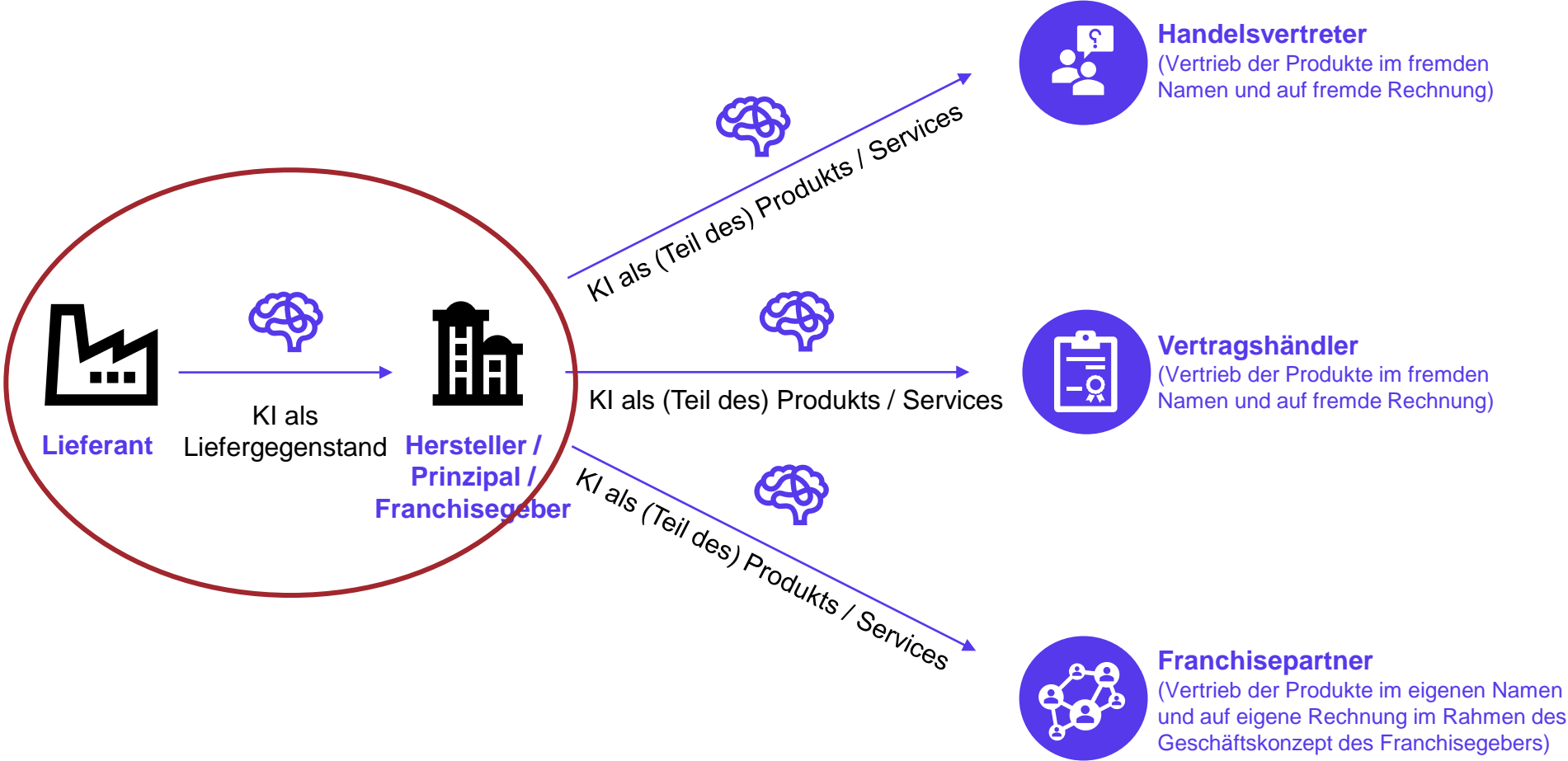


**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Vertragshändler**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

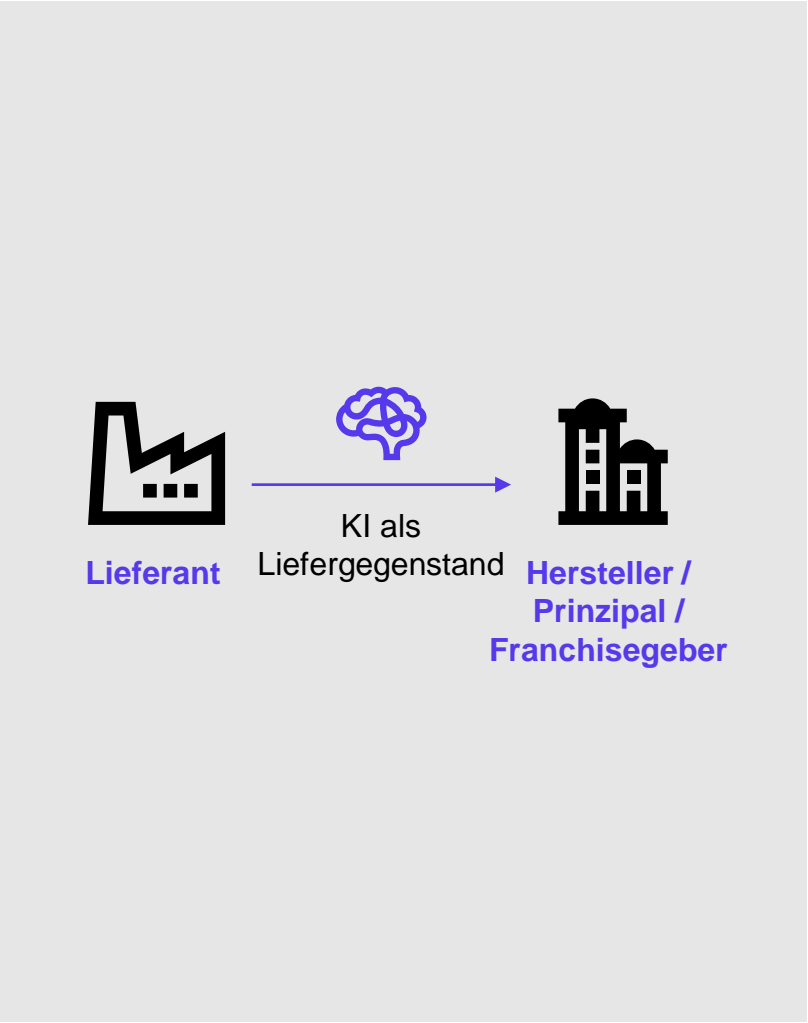
**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)

# KI entlang der Lieferkette – KI als Gegenstand von Produkten / Services





# KI entlang der Lieferkette – KI als Gegenstand von Produkten / Services



## Gegenstand des Sourcing

Daten

KI-System

Speicher / Rechenkapazität

# Risiken beim Sourcing von KI – Data Sourcing




## Personenbezogene Daten





## Immaterialgüterrechtliche geschützte Inhalte



## Maschinengenerierte Daten

-  Urheberrecht
-  Geschmacksmuster- und Designschutzrecht
-  Patentrecht)
-  Markenrecht
-  Sui-generis-Recht des Datenbankherstellers

-  Aufwändige Lizenzierung
-  Zukünftig: Datenlizenz nach dem Data Act



Zukünftig: Anforderungen nach dem AI Act (z.B. Data Governance nach Art. 10 AI Act für Hochrisiko-KI).

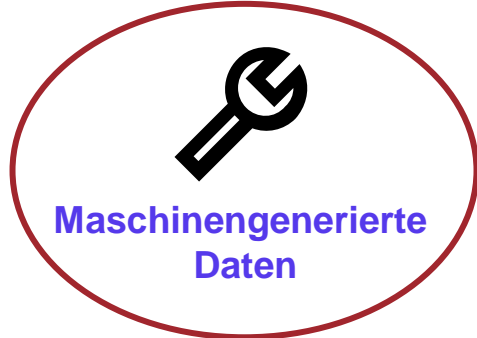
# Risiken beim Sourcing von KI – Data Sourcing



Personenbezogene Daten



Immaterialgüterrechtliche geschützte Inhalte



Maschinengenerierte Daten

- © Urheberrecht
- 📦 Geschmacksmuster- und Designschutzrecht
- 💡 Patentrecht)
- TM Markenrecht
- 📄 Sui-generis-Recht des Datenbankherstellers

- ⚠️ Aufwändige Lizenzierung
- ⚠️ Zukünftig: Datenlizenz nach dem Data Act

 **Zukünftig: Anforderungen nach dem AI Act (z.B. Data Governance nach Art. 10 AI Act für Hochrisiko-KI).**

# Risiken beim Sourcing von KI – Data Sourcing

Immaterialgüterrechtlich geschützter Gegenstand:

- **Ohne Lizenz kein Nutzungsrecht**
- **Datenlizenz:**
  - **Untersagung bestimmter Verwertungshandlungen**
  - **Rein schuldrechtlicher Natur**
    - Hohe Bedeutung von Vertragsstrafen/  
Haftungsregelungen bei Zuwiderhandlungen

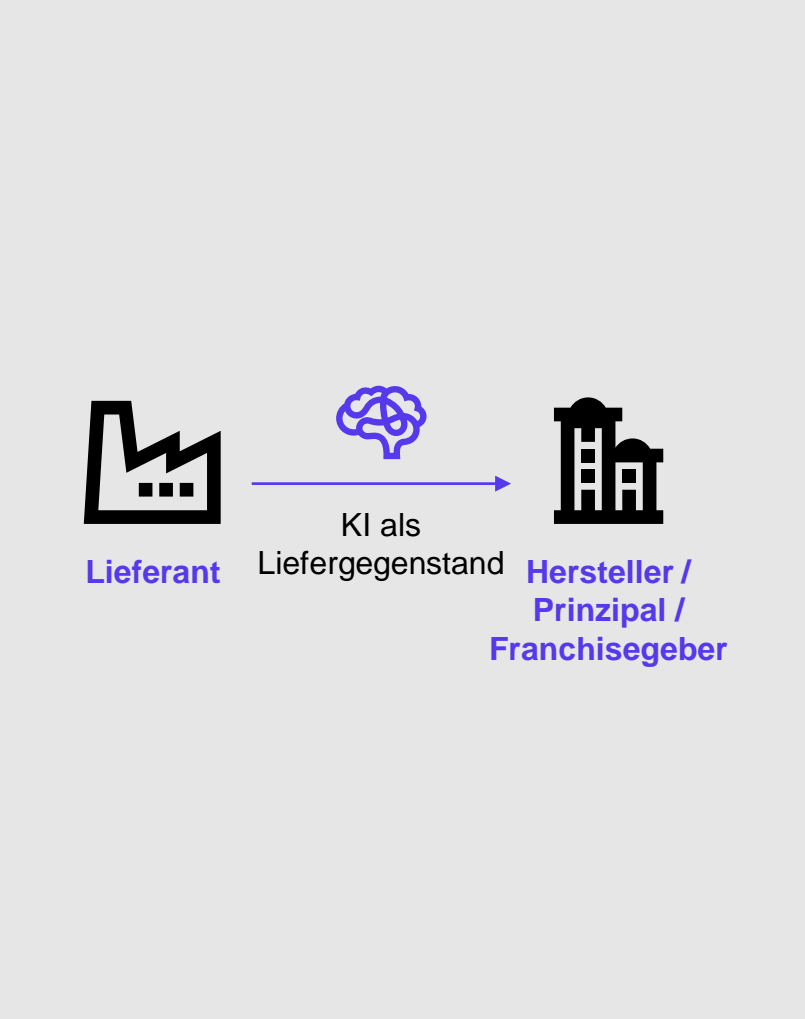
# Risiken beim Sourcing von KI – Data Sourcing

Immaterialgüterrechtlich geschützter Gegenstand:

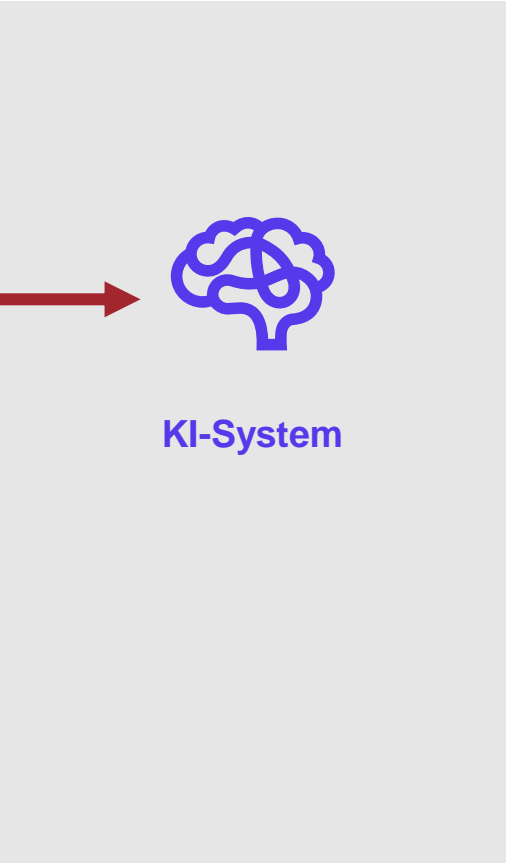
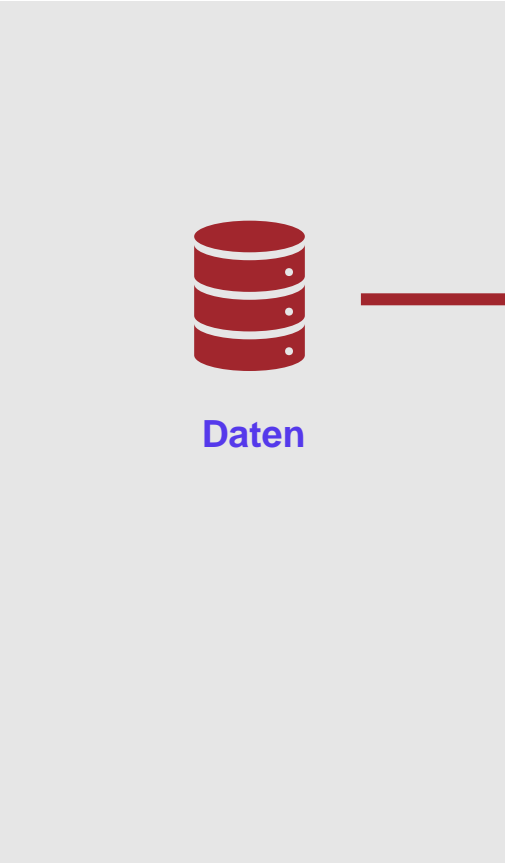
- **Ohne Lizenz kein Nutzungsrecht**
- **Datenlizenz:**
  - **Untersagung bestimmter Verwertungshandlungen**
  - **Rein schuldrechtlicher Natur**
    - Hohe Bedeutung von Vertragsstrafen/  
Haftungsregelungen bei Zuwiderhandlungen



# KI entlang der Lieferkette – KI als Gegenstand von Produkten / Services



## Gegenstand des Sourcing



# Risiken beim Sourcing von KI – Best Practices zur Vertraulichkeit

## Insourcing von Daten:

Vertraulichkeitsvereinbarungen können einer umfassenden Verwertung entgegenstehen



## Training / Nutzung eigener Daten

Vertraulichkeitsbestimmungen zum Schutz eigener Trainings- / Anwenderdaten

- Schutz nach **GeschGehG**
- Vermeidung eines Verstoßes gegen **Vertraulichkeitsvereinbarung mit Dritten**



## Best Practices



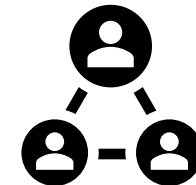
### Vertraglich

- Keine Wiederverwendung von Inhalten durch Provider (Prompts, Output)
- sowie Weitergabe an Dritte untersagt
- Vertragsstrafen / Haftungsregelungen



### Technisch

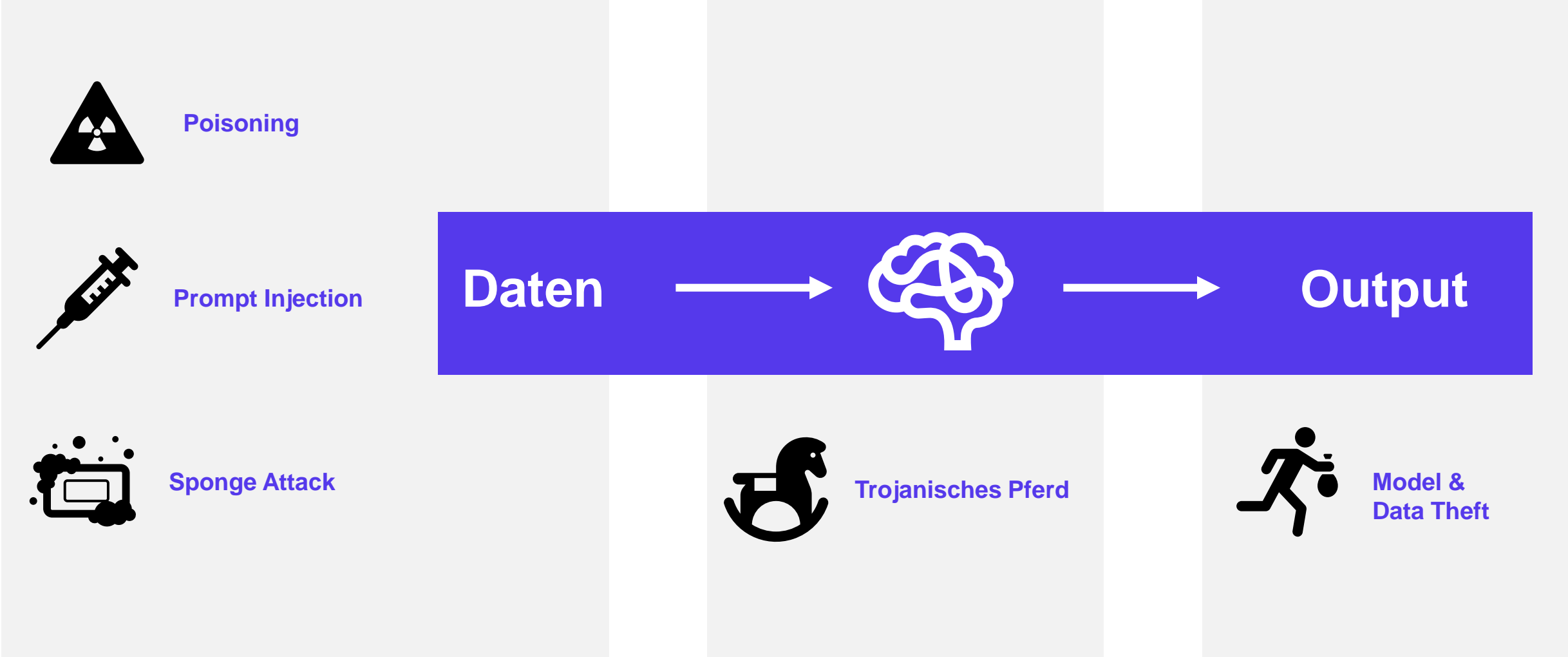
- Eigene Instanz / off-premise
- Monitoring / Verschlüsselung
- Tags



### Organisatorisch

- Interne Maßnahme: Compliance
- Regelungen / Guidelines zur Verwendung von AI im Unternehmen

# Risiken beim Sourcing von KI – Datensicherheit / Cybersecurity





# Risiken beim Sourcing von KI – KI Qualität

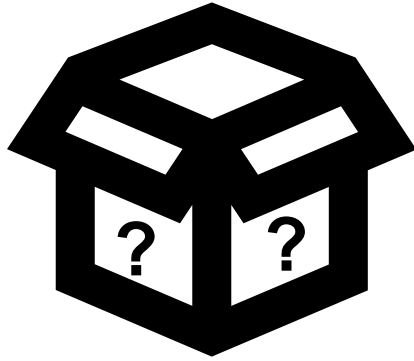
Verfügbarkeiten (SLA)	Leistungsfähigkeit und Kompensation	Kompatibilität	Verwendbarkeit der Ergebnisse	Datenqualität?
Reaktionszeiten KPIs	Token-basierte Abrechnung	Verantwortungs- abgrenzung Nutzungsart	„fit for purpose“	Human Oversight  Halluzinationen, Model Drift



## Best Practices:

- Möglichst **detaillierte Beschreibung des Vertragsgegenstandes** und der Nutzungsart
- Festlegung von **SLs und KPIs**
- Abstimmung des eigenen **Business Concepts** mit Kapazität
- Interne **Compliance-Richtlinien**, insb. zur Human Oversight

# Model Sourcing – Nachvollziehbarkeit



**Black Box**

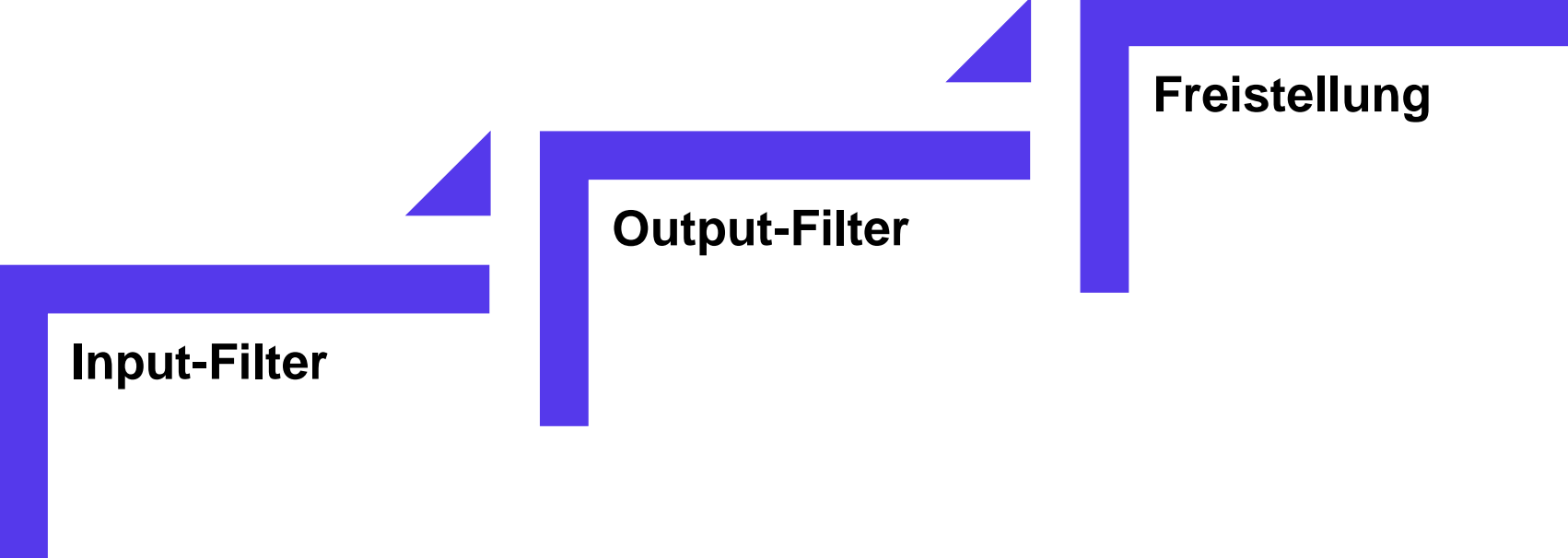
## Problemfelder:

- Mangelnde **Transparenz**
- Algorithmische **Verzerrungen** ("Model Drift")
- **Parameter und Gewichtungen**
- **Datenquellen**
- Regulatorische Anforderungen

## Best Practices:

- **Visualisierungswerkzeuge**
- **Detaillierte Logs und Dokumentation**
- **Regelmäßige Überprüfung und Validierung**

# Model Sourcing – Verletzung von Rechten Dritter



# KI-Sourcing – Vertragliche Aspekte aus Kundensicht

## Nachvollziehbarkeit

- Visualisierung
- Logs / Dokumentation

## Technische Aspekte

- Leistungsfähigkeit / Qualität des Modells (FLOPS, Inferenzzeit)

## Usability

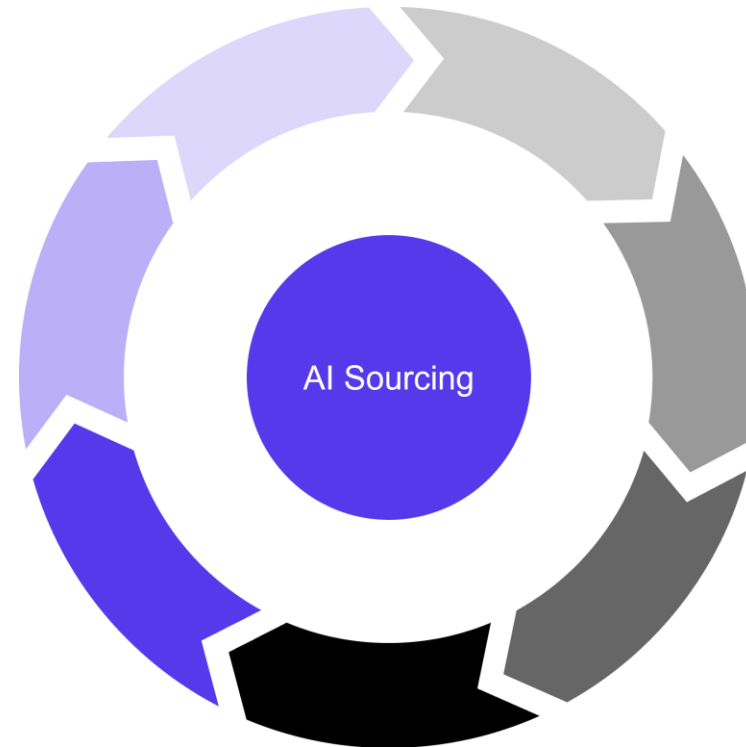
- Einfaches Konfigurieren eigener Use Cases möglich

## Maintenance

- Model Drift

## Leistungsbeschreibung

- Definition von KPIs/ SLAs
- (z. B. Wahrscheinlichkeitsangaben)
- Schnittstellen APIs, Kompatibilität
- Maßnahmen gegen Halluzinationen, Model Drift (Aktualität der Daten, Refresh)



## Vertraulichkeit

- Eigene Instanz / off-premise, Mandantenfähigkeit
- Geschäftsgeheimnisgesetz
- Monitoring / Verschlüsselung

## Lizenzmodell (Nutzungs- / Urheberrechte)

- Schuldrechtliche Allokation des KI-Outputs / trainierten Modells
- Keine Wiederverwendung von Inhalten durch Provider (Prompts, Output)
- Haftungsfreistellung für die Verletzung von Rechten Dritter

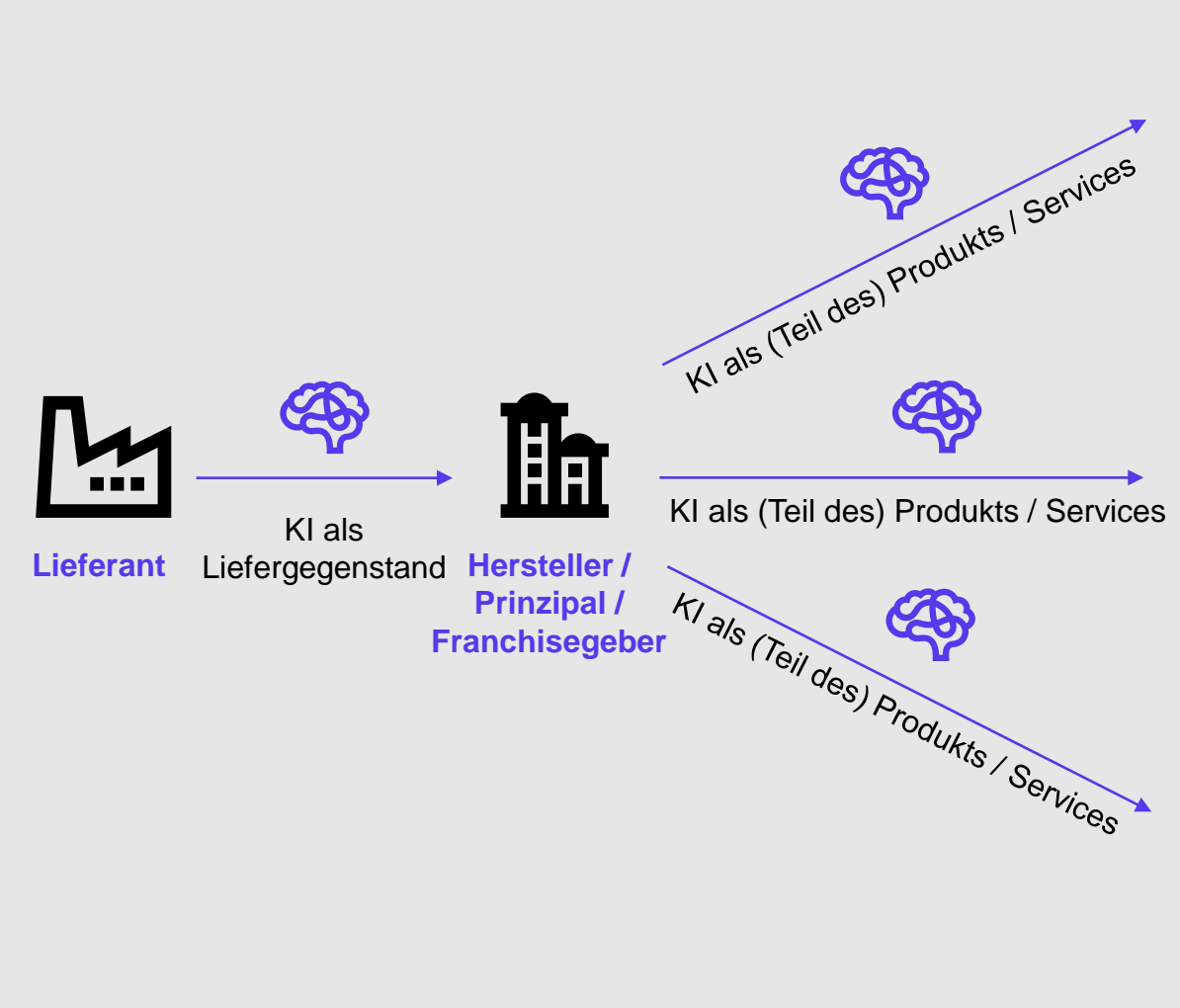
## Trainingsdaten

- Datenlizenz, Data Act, Datenschutz, AGG,
- Datenqualität
- Auskunftsansprüche nach KI-VO
- Immaterialgüterrechtliche Schranken

## Haftung

- Klare Abgrenzung der Verantwortungsbereiche nötig
- Produktsicherheitsverordnung
- Auskunftsanspruch nach KI-VO
- Bußgelder bei Non-Compliance (AI Act, DS-GVO, Data Act)

# KI entlang der Lieferkette – KI als Gegenstand von Produkten / Services

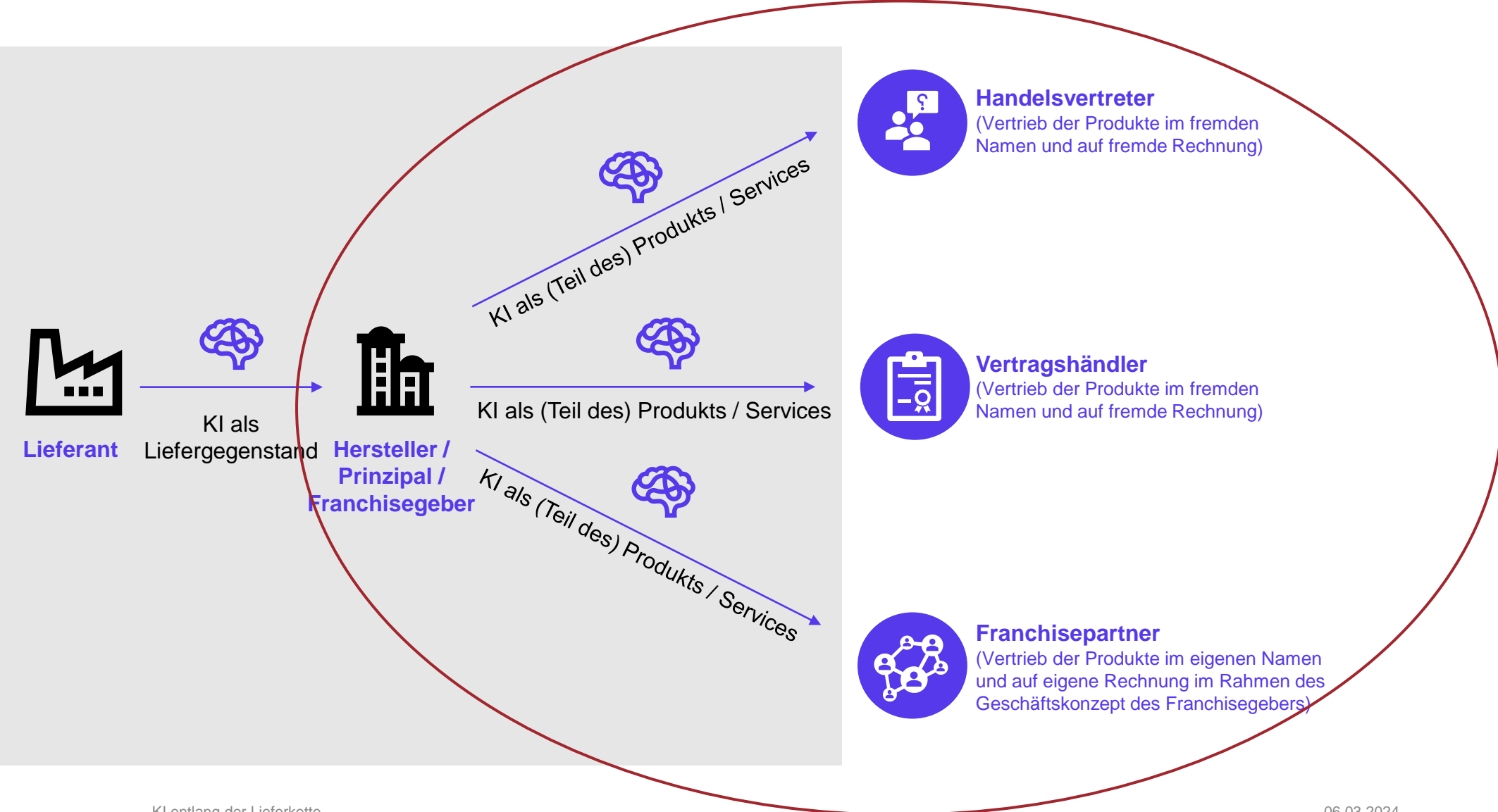


**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

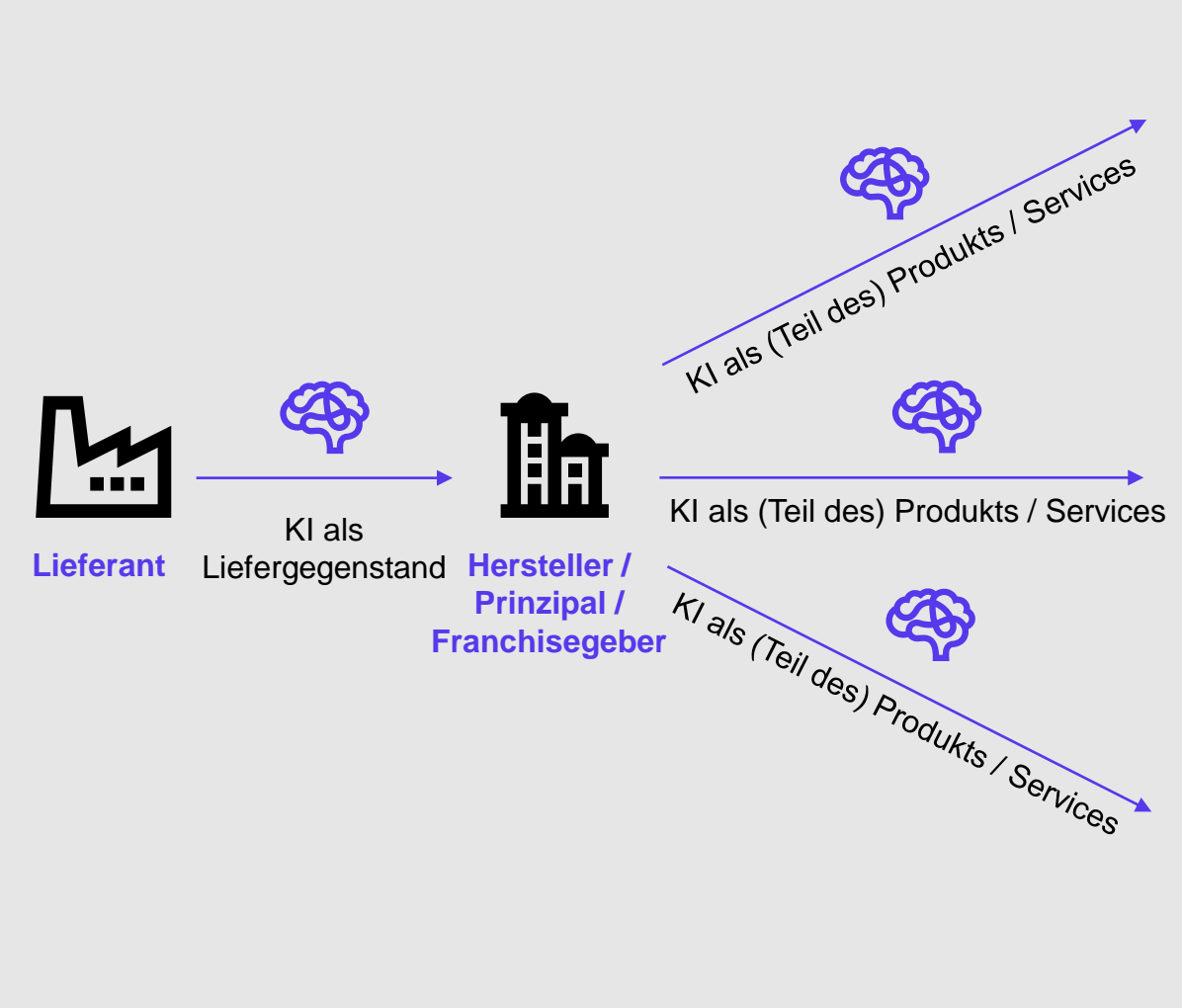
**Vertragshändler**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)

# KI entlang der Lieferkette – KI als Gegenstand von Produkten / Services



# KI entlang der Lieferkette – KI als Gegenstand von Produkten / Services



**Handelsvertreter**  
 (Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Vertragshändler**  
 (Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

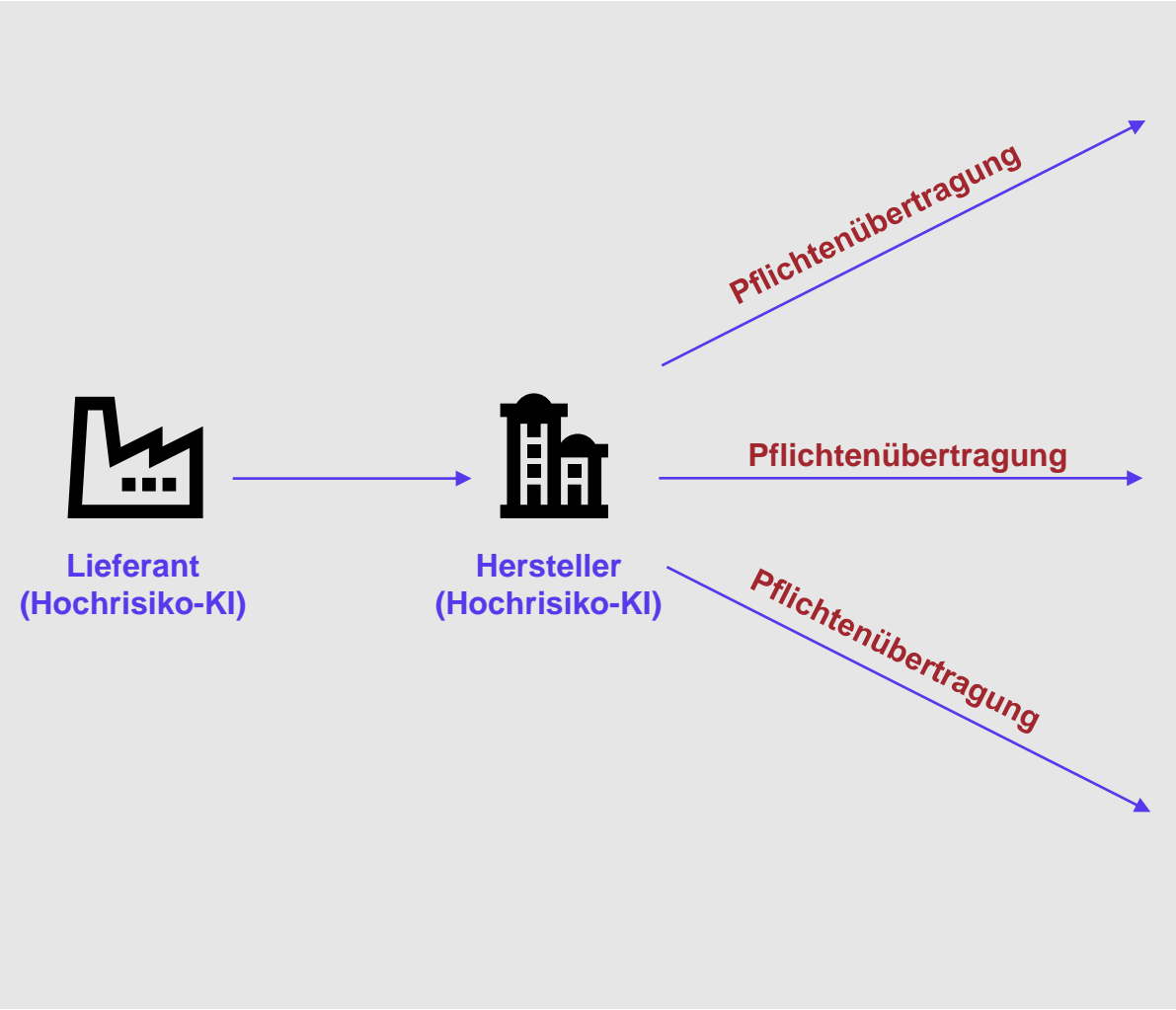
**Franchisepartner**  
 (Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)



**Informationspflichten**  
 (z.B. nach dem Data Act)

**Lizenz/ Recht zur Sublizenzierung**

# Hochrisiko-KI entlang der Lieferkette – Übertragung der Herstellerpflichten nach dem AI Act



**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Vertragshändler**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung)

**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)

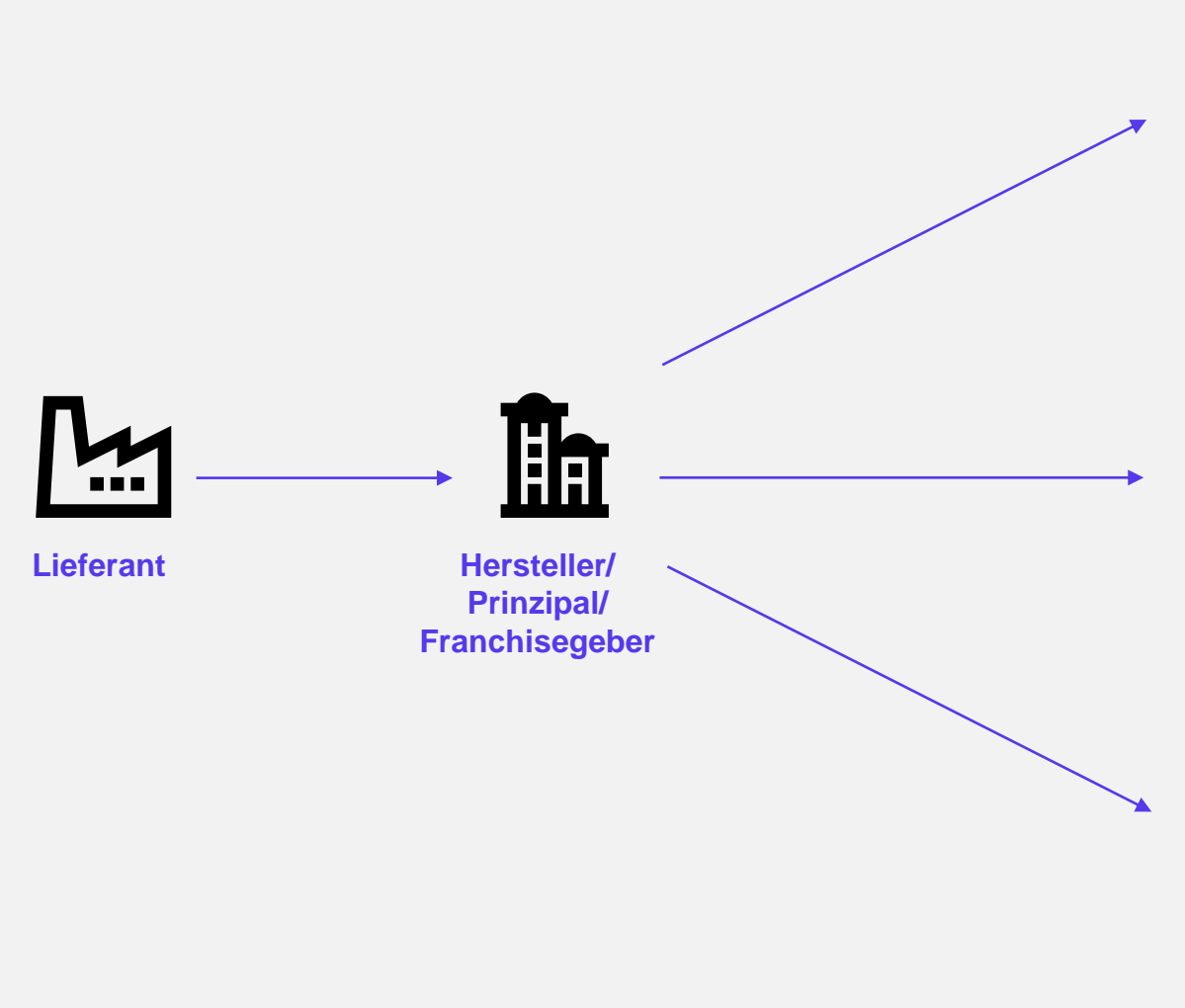
## Übertragungsrisiken

- Anbringung von Markenzeichen oder Namen auf KI**
- Modifizierung von KI-Systemen, unabhängig von Einstufung als Hochrisiko-KI**



# Risiken bei Einsatz von KI

# Einsatz von KI entlang der Lieferkette



**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)



**Vertragshändler**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung)



**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)

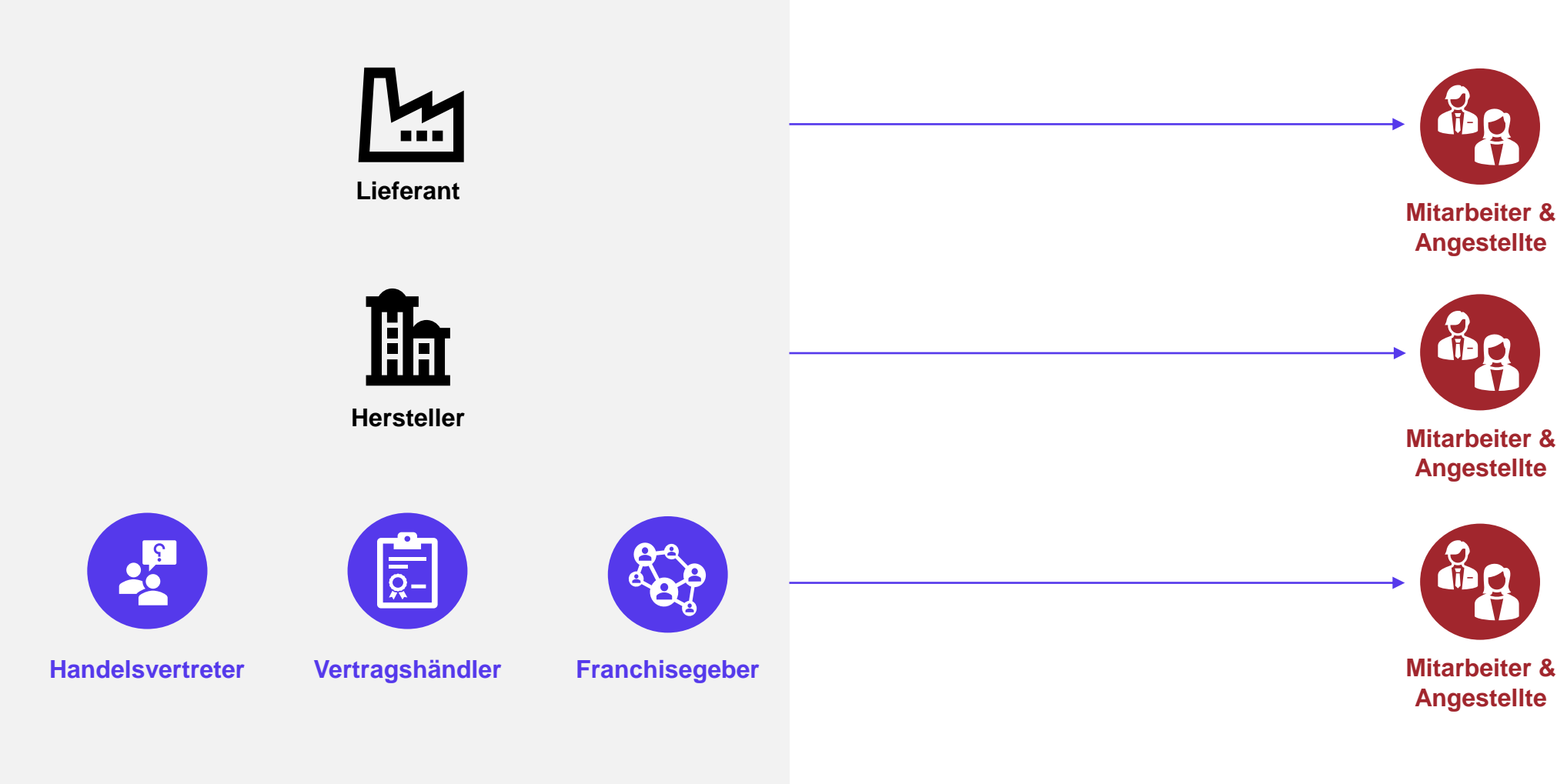
1

**KI Nutzung intern**  
(beispielsweise durch Angestellte & Mitarbeiter)

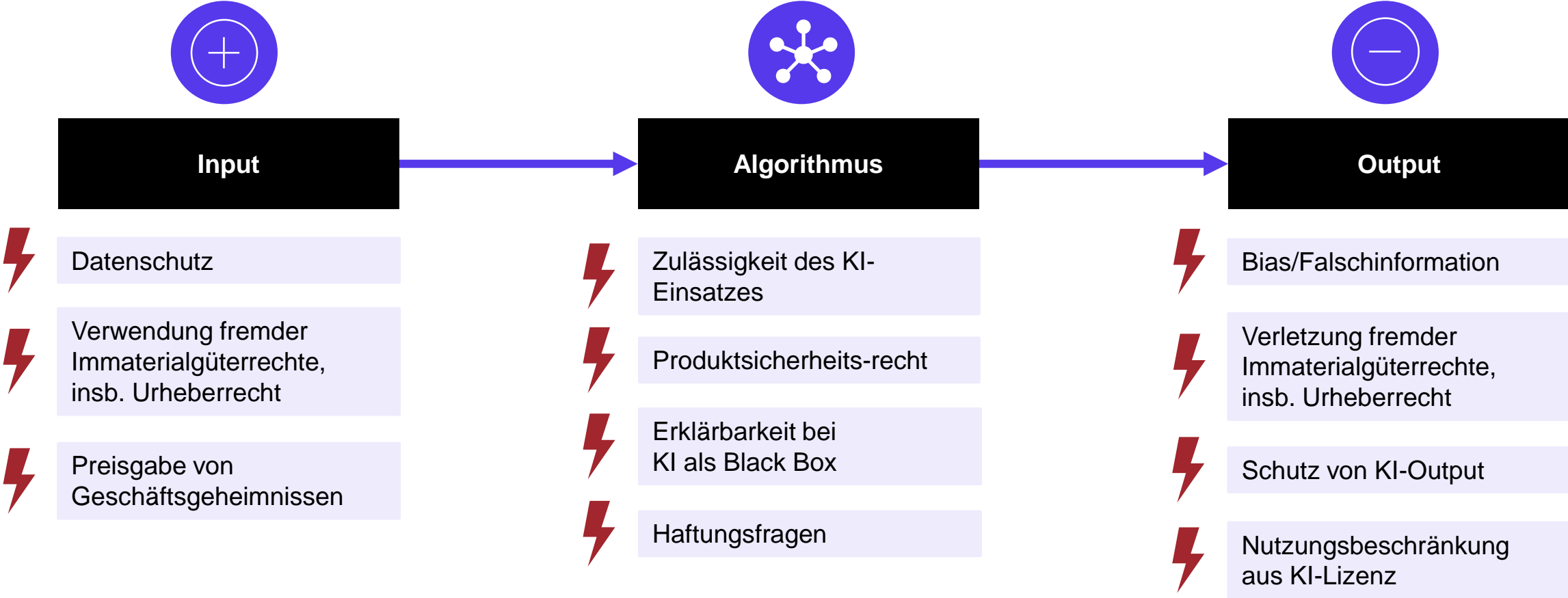
2

**KI Nutzung durch Vertragspartner**  
(beispielsweise Lieferant und Vertriebsmittler)

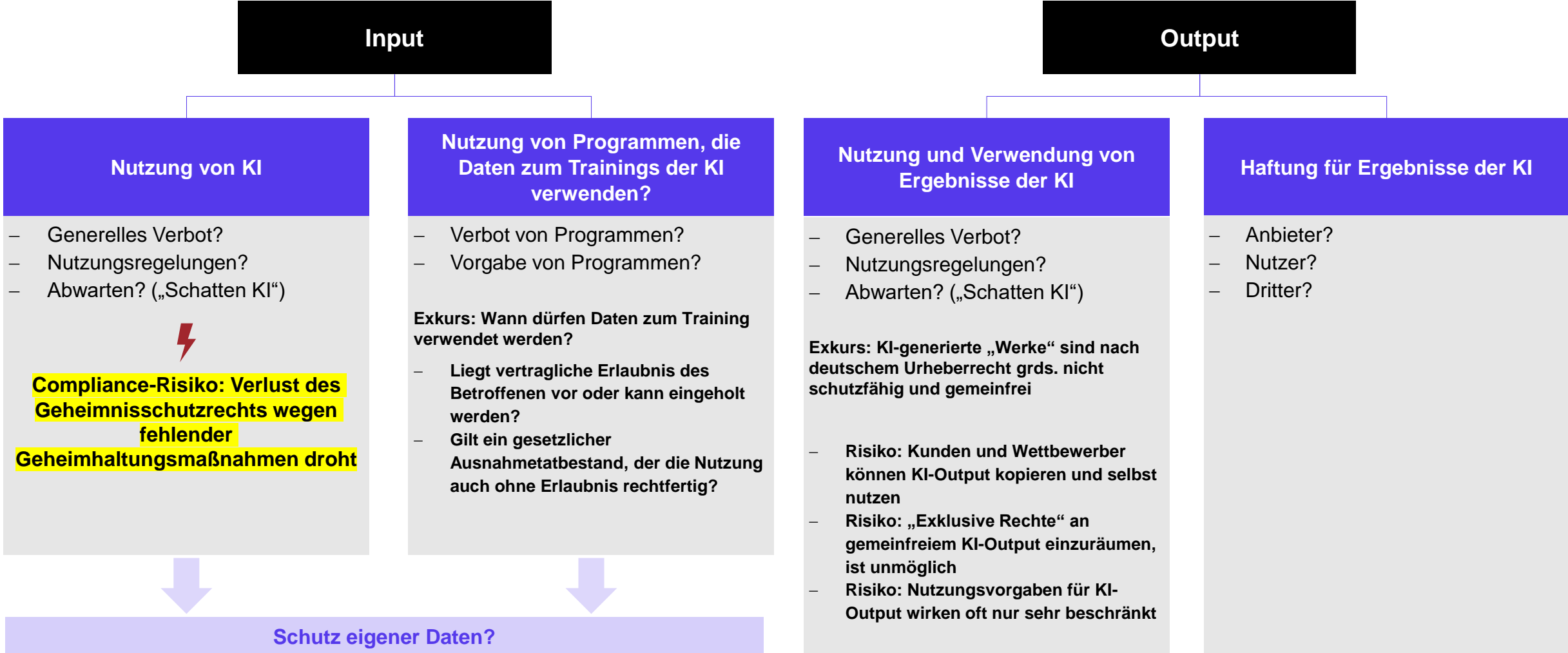
# Einsatz von KI innerhalb der Unternehmen



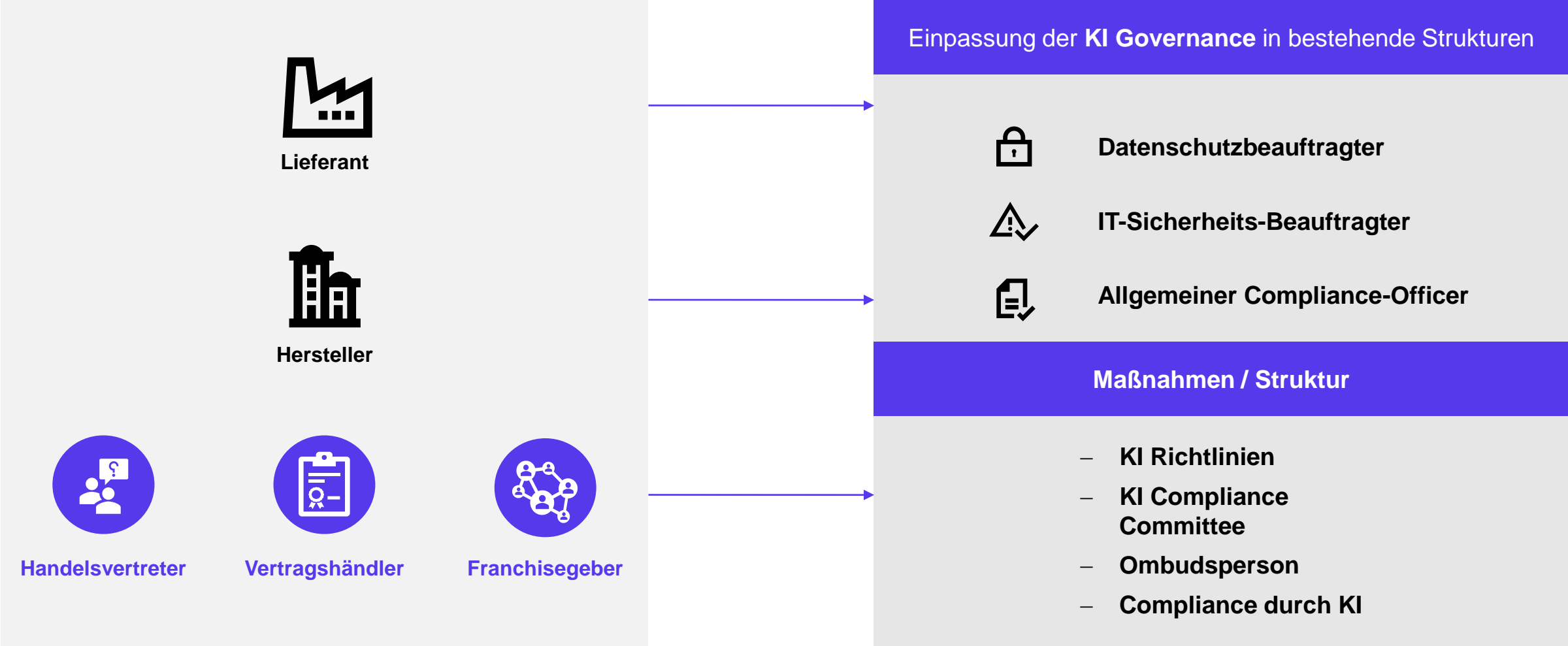
# Rechtliche Risiken beim Einsatz von KI innerhalb von Unternehmen



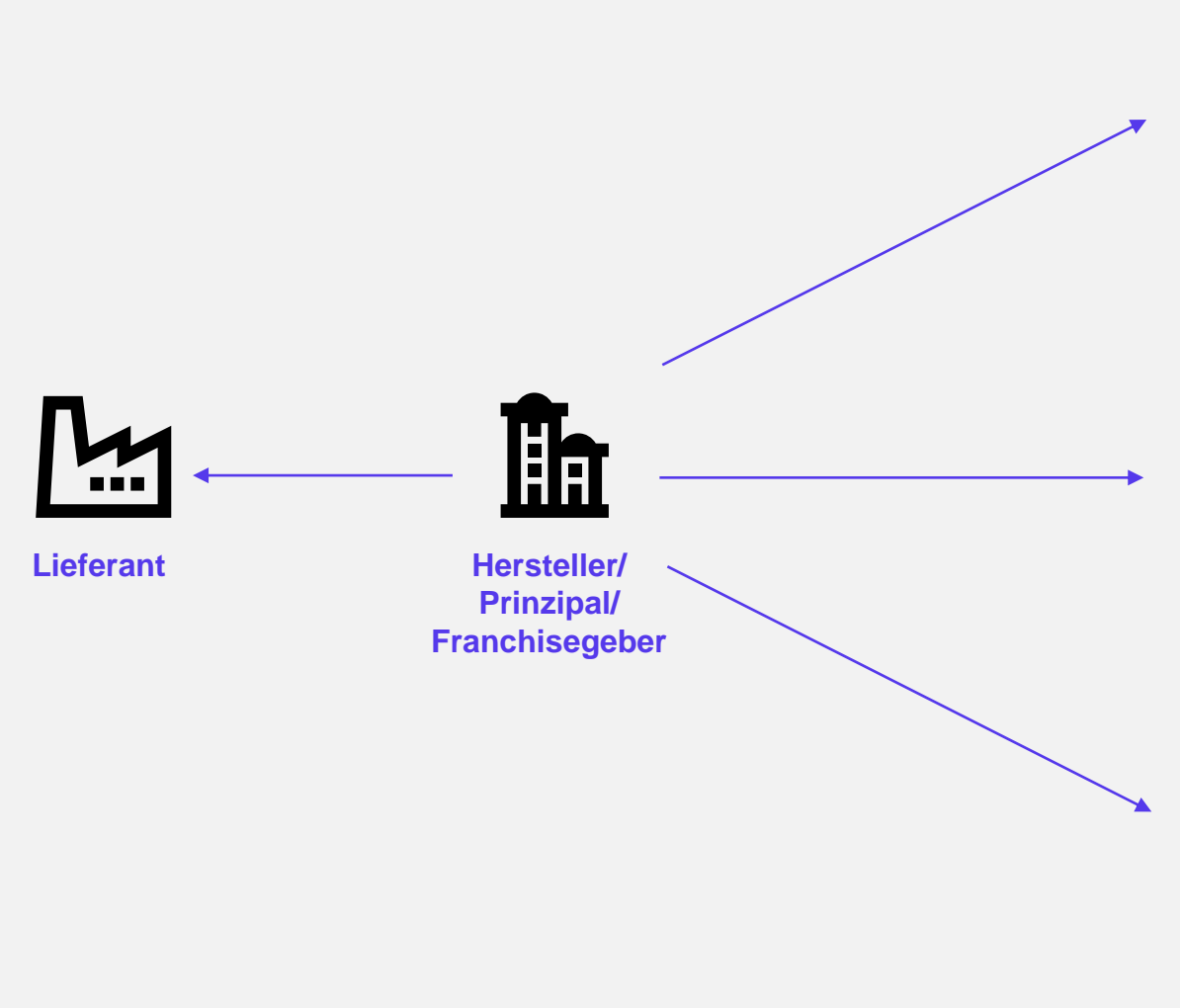
# Rechtliche Risiken beim Einsatz von KI – Deep Dive



# Risikominimierung – KI Governance innerhalb des Unternehmens



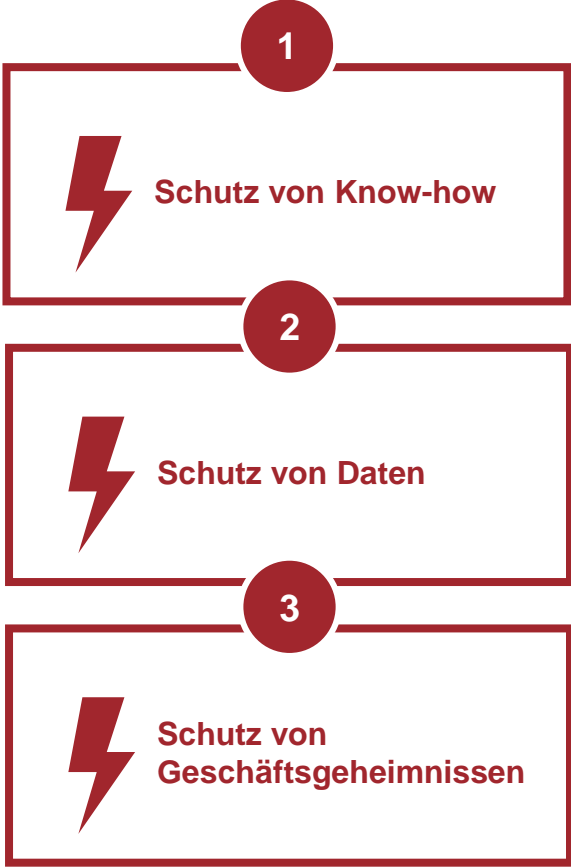
# Einsatz von KI durch Vertragspartner



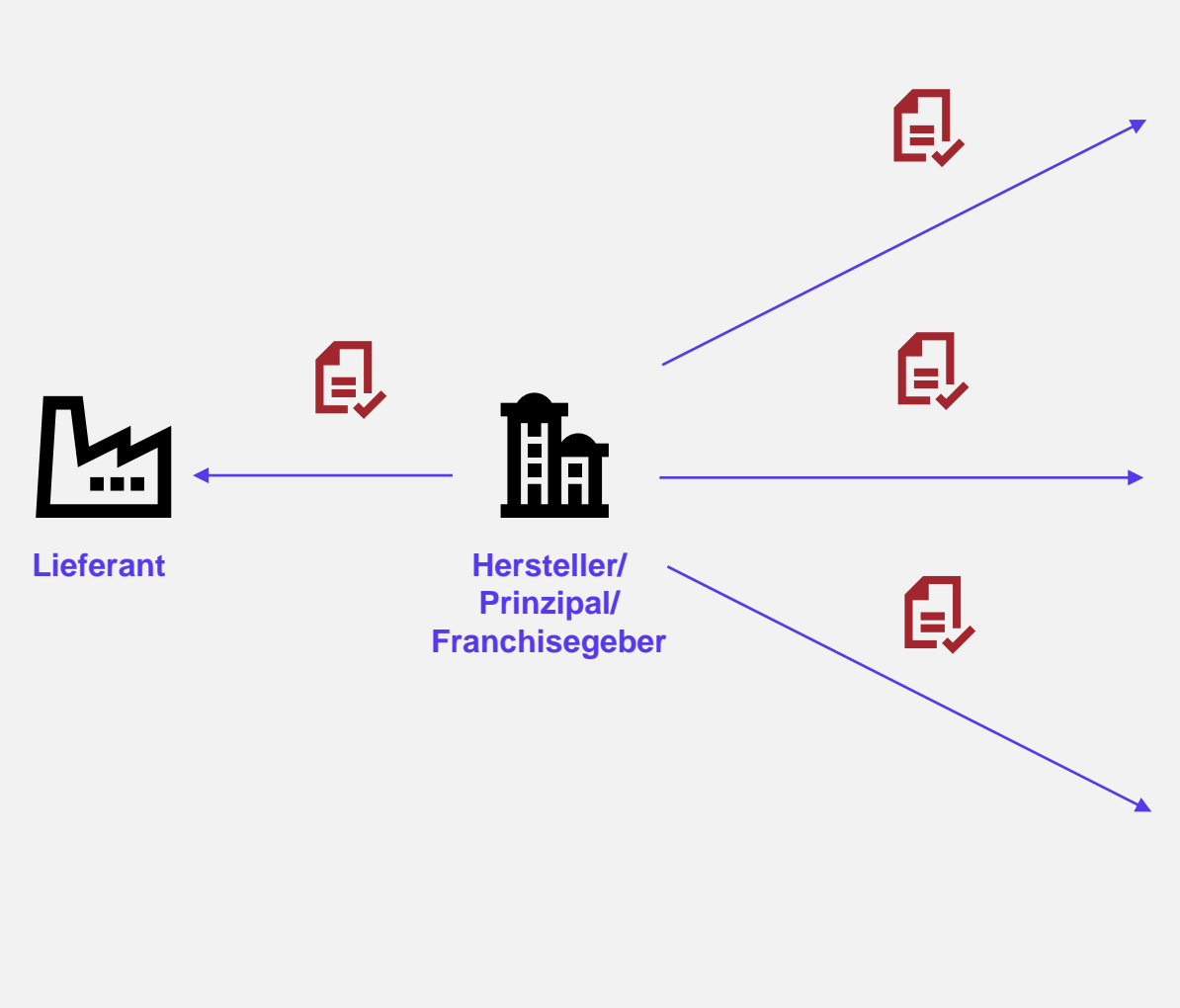
**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Vertragshändler**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung)

**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)



# Risikominimierung – KI Governance gegenüber Vertragspartner



**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Vertragshändler**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung)

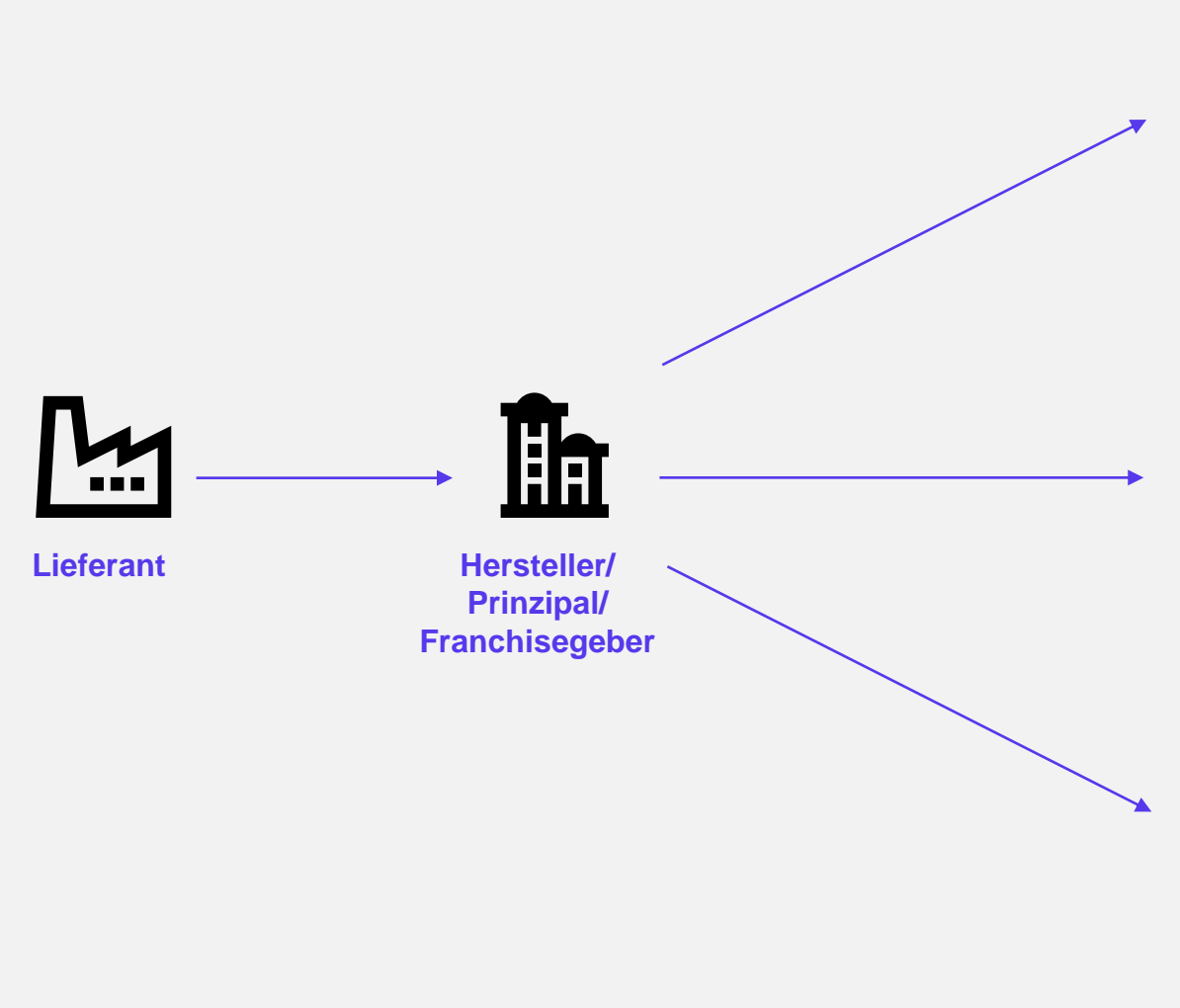
**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)

**Vorgabe zur Nutzung von KI durch KI Richtlinien?**



# Fazit

# Fazit: Einsatz von KI entlang der Lieferkette



**Handelsvertreter**  
(Vertrieb der Produkte im fremden Namen und auf fremde Rechnung)

**Vertragshändler**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung)

**Franchisepartner**  
(Vertrieb der Produkte im eigenen Namen und auf eigene Rechnung im Rahmen des Geschäftskonzept des Franchisegebers)

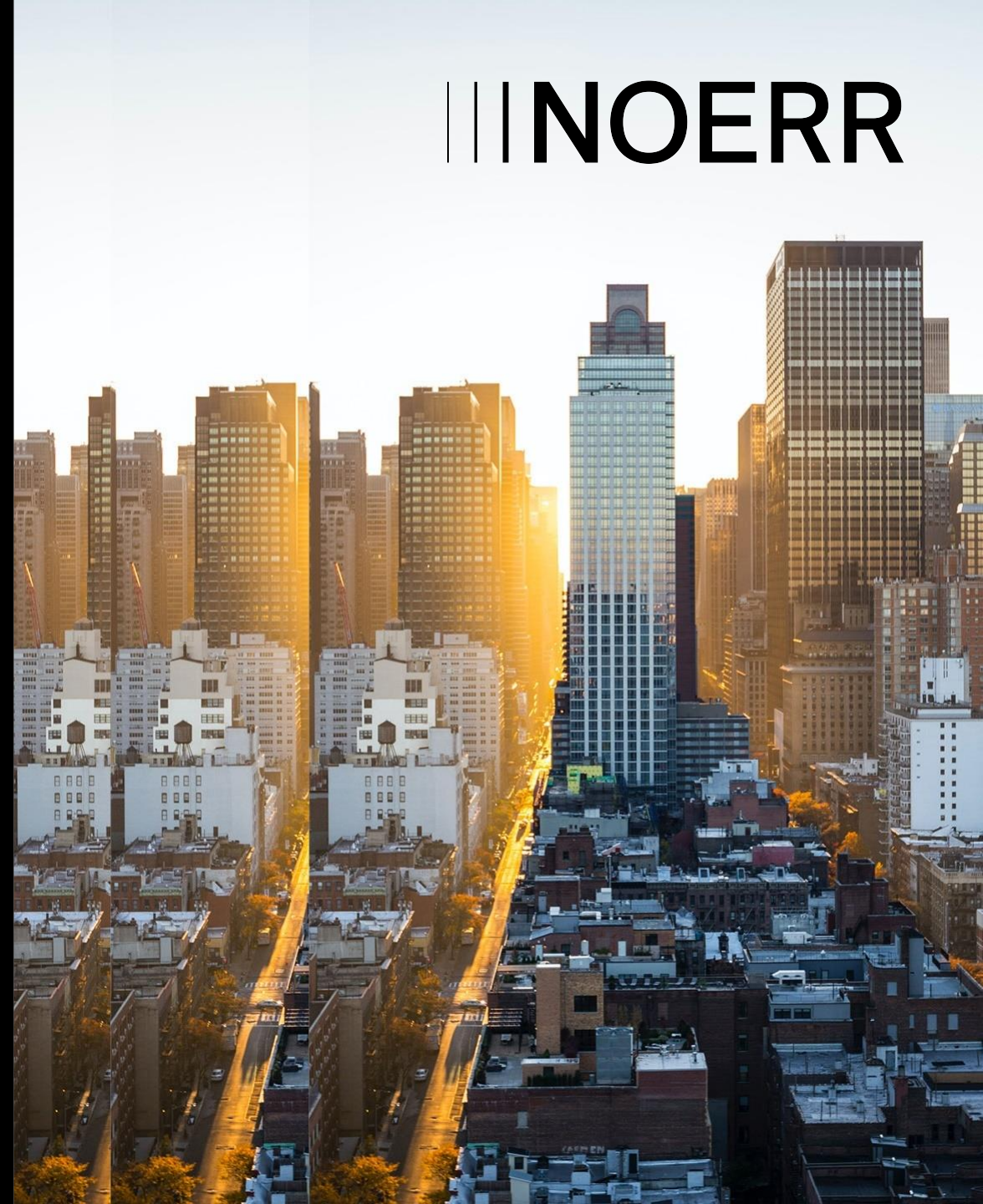
1

**KI Sourcing: KI als Gegenstand Vertragsprodukten oder Dienstleistungen**

2

**Einsatz von KI durch „Player“ der Lieferkette**

||| NOERR



info@noerr.com  
noerr.com  
© Noerr PartGmbB

# Referentinnen



## **Marieke Merkle**

Rechtsanwältin

Associated Partner

+49 89 28628 227

marieke.merkle@noerr.com

Marieke Merkle ist spezialisiert auf die rechtliche Beratung im Bereich Data Economy (insbesondere Cloud-Computing, Datennutzungsverträge, KI) sowie auf die rechtliche Beratung im Zusammenhang mit Digitalisierungsprojekten nationaler und internationaler Mandanten (insbesondere Automatisierung von Unternehmensprozessen, IT-Projekte, IT-Outsourcings) und Softwareurheberrecht (einschließlich Open Source Software). Marieke Merkle ist Lehrbeauftragte an der LMU München für IT-Recht.

### **Ausgewählte Publikationen**

- Outbound-Compliance: Aktive Beteiligung an Open-Source-Projekten, MMR 2022, 251
- Der Entwurf des Data Acts, Recht Digital RDi 2022, 168 (zusammen mit Dr. David Bomhard)
- Regulation of Artificial Intelligence – The EU Commission’s proposal of an AI Act, EuCML 2021, 257 (zusammen mit Dr. David Bomhard)
- Europäische KI-Verordnung: Der aktuelle Kommissionsentwurf und praktische Auswirkungen, Recht Digital RDI 2021, 276-283 (zusammen mit Dr. David Bomhard)
- Regelmäßige Beiträge in ROBOTIK UND PRODUKTION

# Referentinnen



## Dr. Jasmin Schulzweida

Rechtsanwältin  
Senior Associate

+49 40 300397145

jasmin.schulzweida@noerr.com

Jasmin Schulzweida ist spezialisiert auf die rechtliche Beratung im Vertriebsrecht im Bereich der Automobil- und Konsumgüterindustrie sowie im Franchiserecht. Sie berät und vertritt nationale und internationale Mandanten in allen vertriebsrechtlichen Fragen, insbesondere bei der Gestaltung und Verhandlung von Vertriebs-, Liefer- und Franchiseverträgen. Darüber hinaus berät und vertritt sie bei der Durchsetzung von Ansprüchen in der Lieferkette. Jasmin Schulzweida veröffentlicht regelmäßig zu vertriebsrechtlichen Themen.

### Ausgewählte Publikationen

- Franchise Agreement, in: Pfaff (Hrsg.), Lizenzverträge – Formulkommentar, Beck-Verlag, 4. Auflage (zusammen mit Prof. Dr. Karsten Metzloff)
- Zur Wirksamkeit insolvenzabhängiger Lösungsklauseln in Vertriebsverträgen, ZVertriebsR 2024, 71
- Social Media Guidelines in Franchisesystemen, ZVertriebsR 2023, 3 (zusammen mit Prof. Dr. Karsten Metzloff)
- International Comparative Legal Guide - Franchise 2024, Chapter Germany (zusammen mit Dr. Tom Billing)
- The Franchise Law Review: Germany, 10<sup>th</sup> Edition, Chapter Germany (zusammen mit Prof. Dr. Karsten Metzloff)
- Regelmäßige Beiträge in ZVertriebsR und ILO Franchise Newsletter