

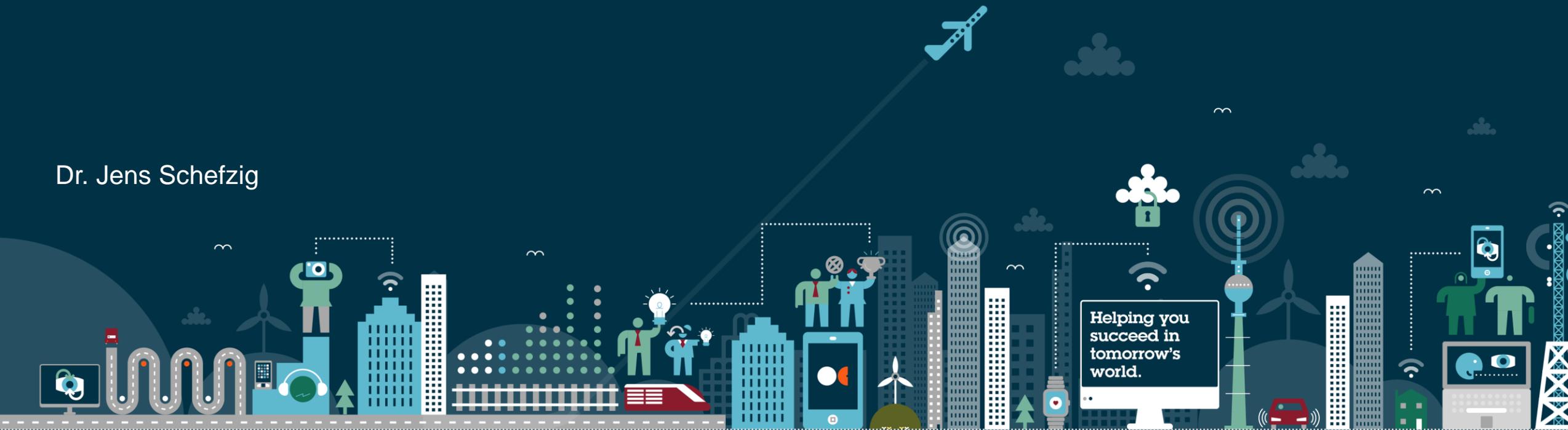
Digitale Geschäftsmodelle im Maschinenbau

Rechtliche Komplexität managen



31. Mai 2023

Dr. Jens Schefzig



Contents

- 01 Komplexität durch das multipolare Geschäftsmodell

- 02 Komplexität durch bestehende Regulierung

- 03 Komplexität durch kommende Regulierung

- 04 Management der Komplexität in Verträgen und Prozessen



Contents

- 01** **Komplexität durch das multipolare Geschäftsmodell**

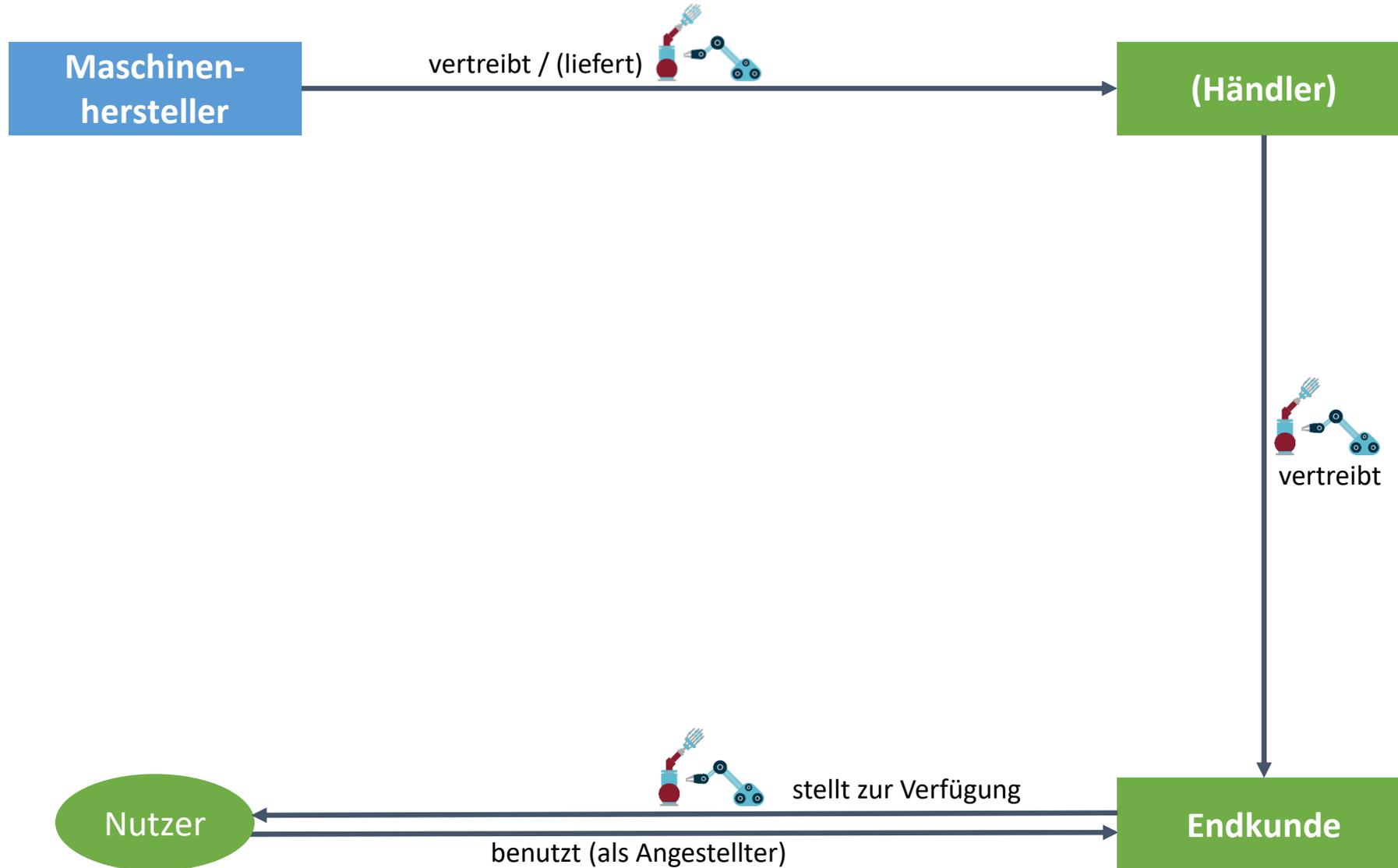
- 02 Komplexität durch bestehende Regulierung

- 03 Komplexität durch kommende Regulierung

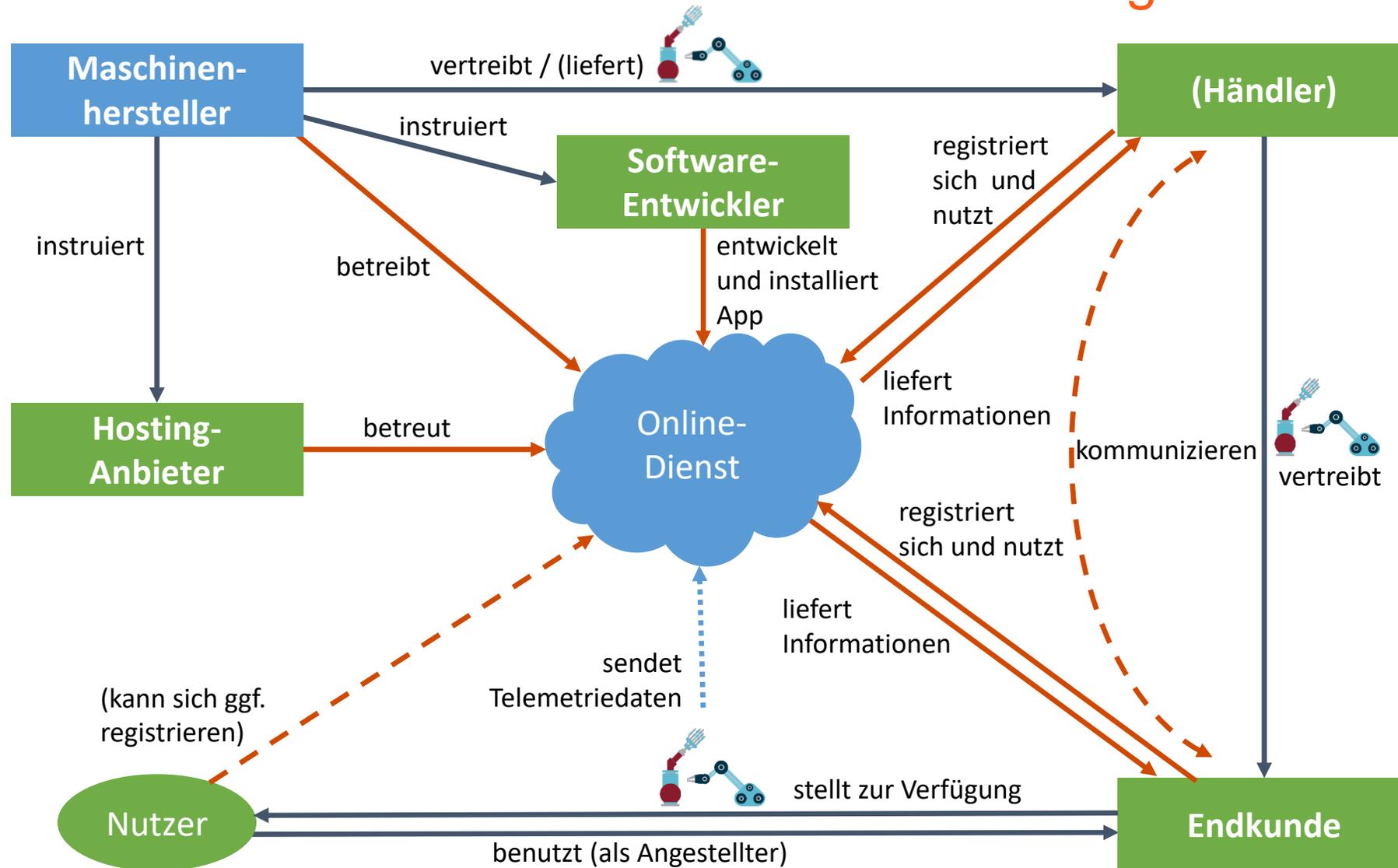
- 04 Management der Komplexität in Verträgen und Prozessen



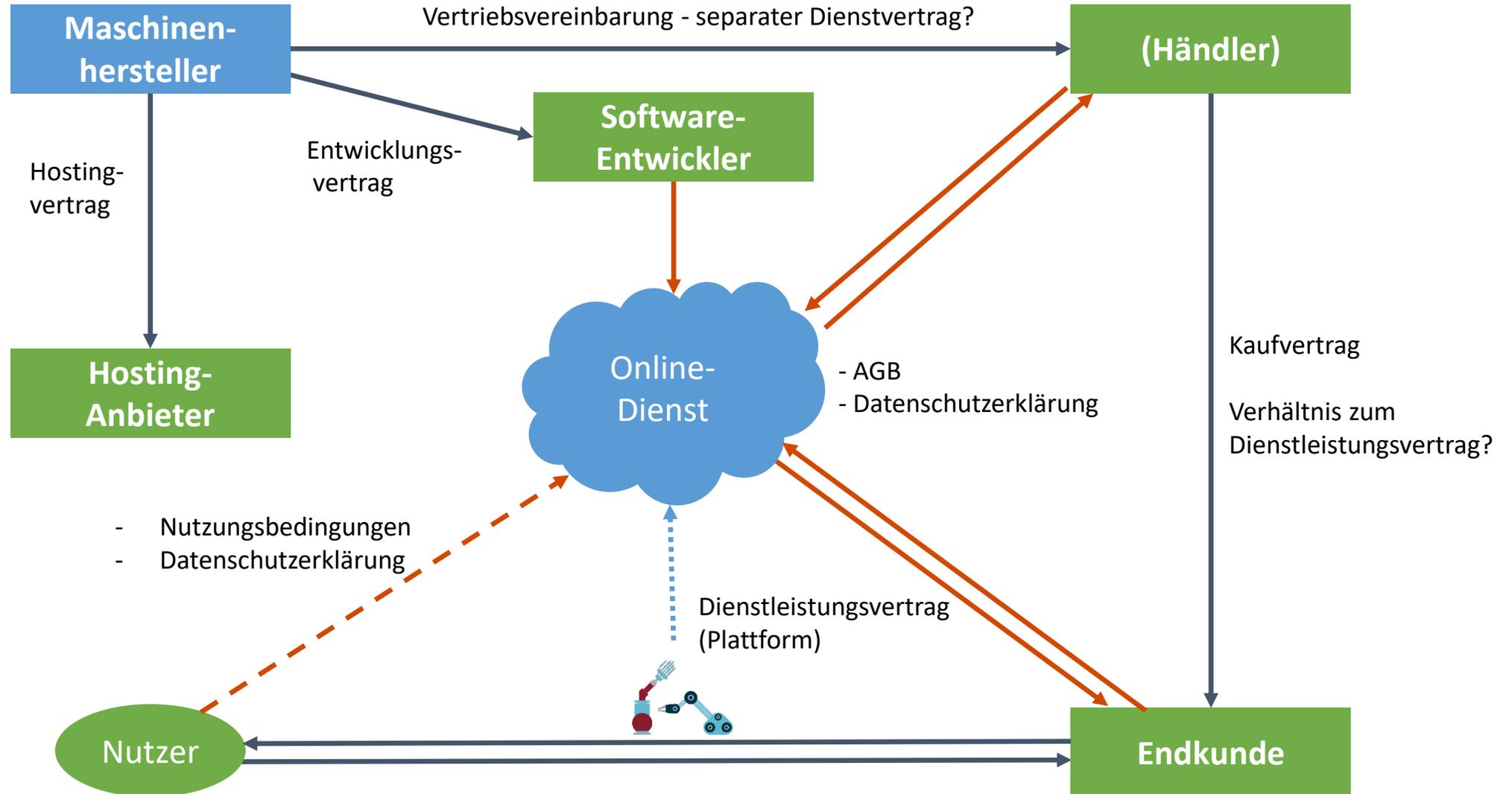
Traditionelles Geschäftsmodell: Produktion von Maschinen



Digitale Transformation: Wie ändert sich die Rechtslage?



Welche Rechtstexte sind für das neue Geschäftsmodell notwendig?



Contents

- 01 Komplexität durch das multipolare Geschäftsmodell

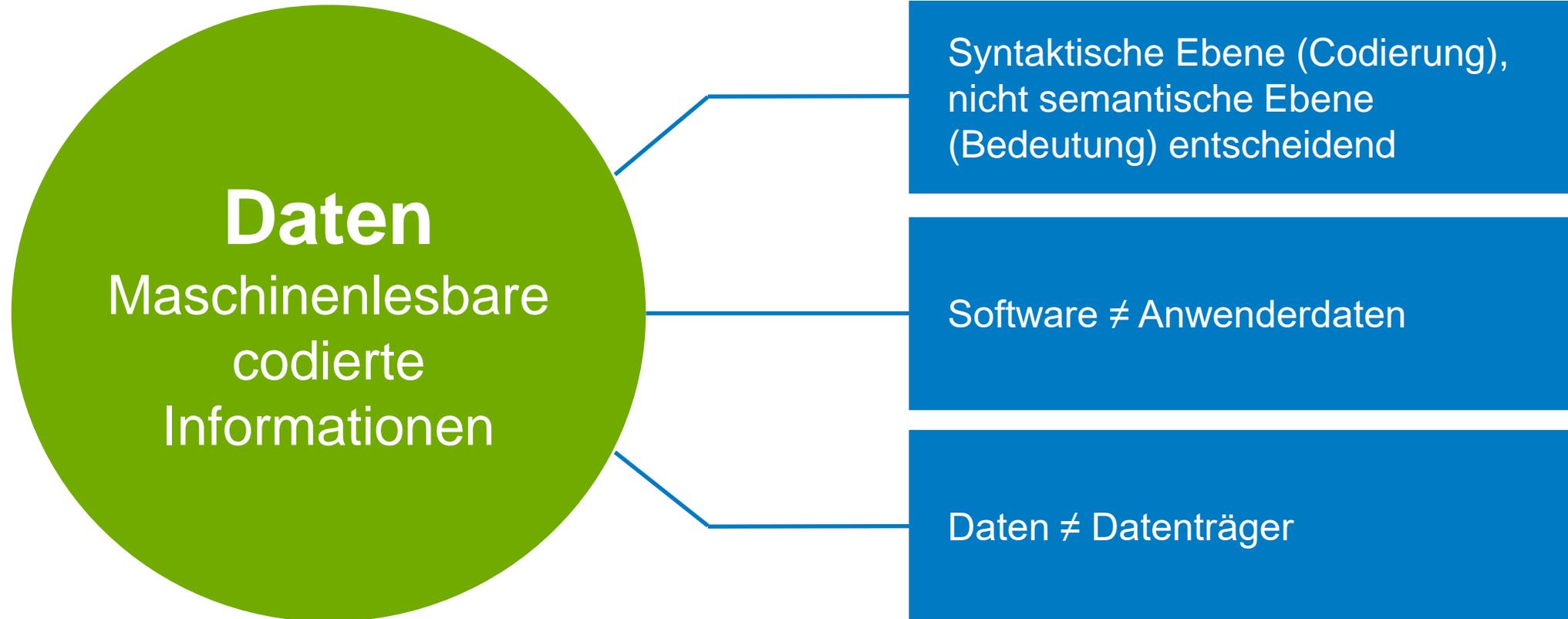
- 02 Komplexität durch bestehende Regulierung**

- 03 Komplexität durch kommende Regulierung

- 04 Management der Komplexität in Verträgen und Prozessen

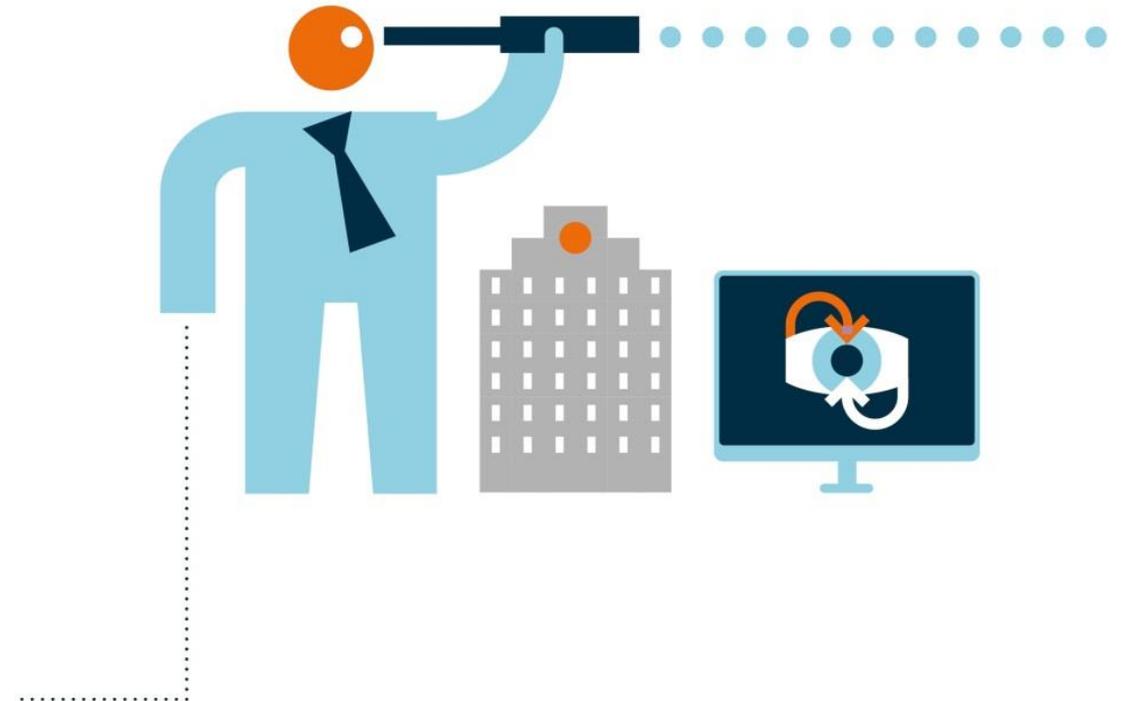


Der Begriff der Daten



Fazit

Ein verlässliches Recht an Daten existiert nicht!

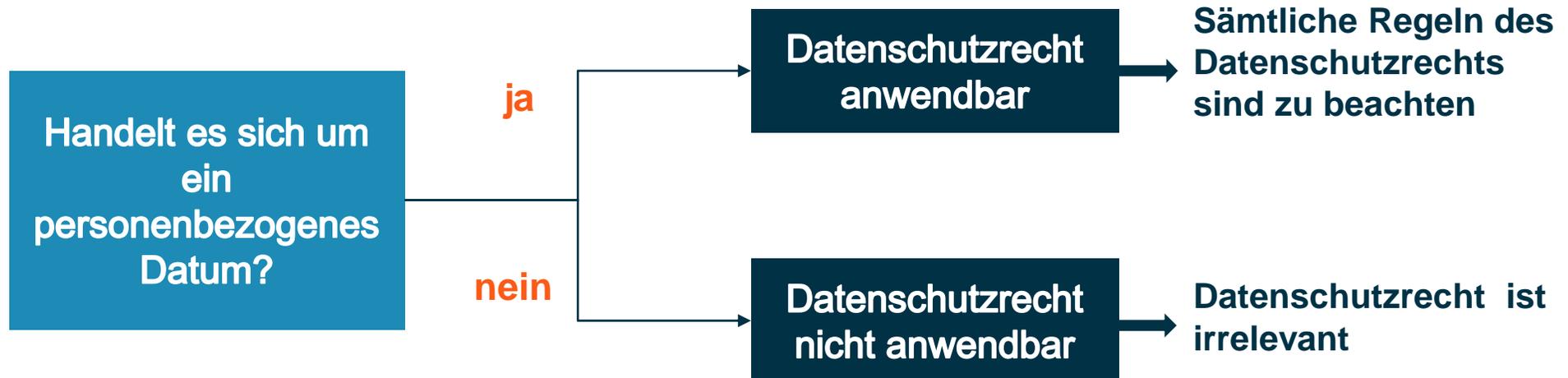


Absicherung von Daten durch vertragliche Regelungen

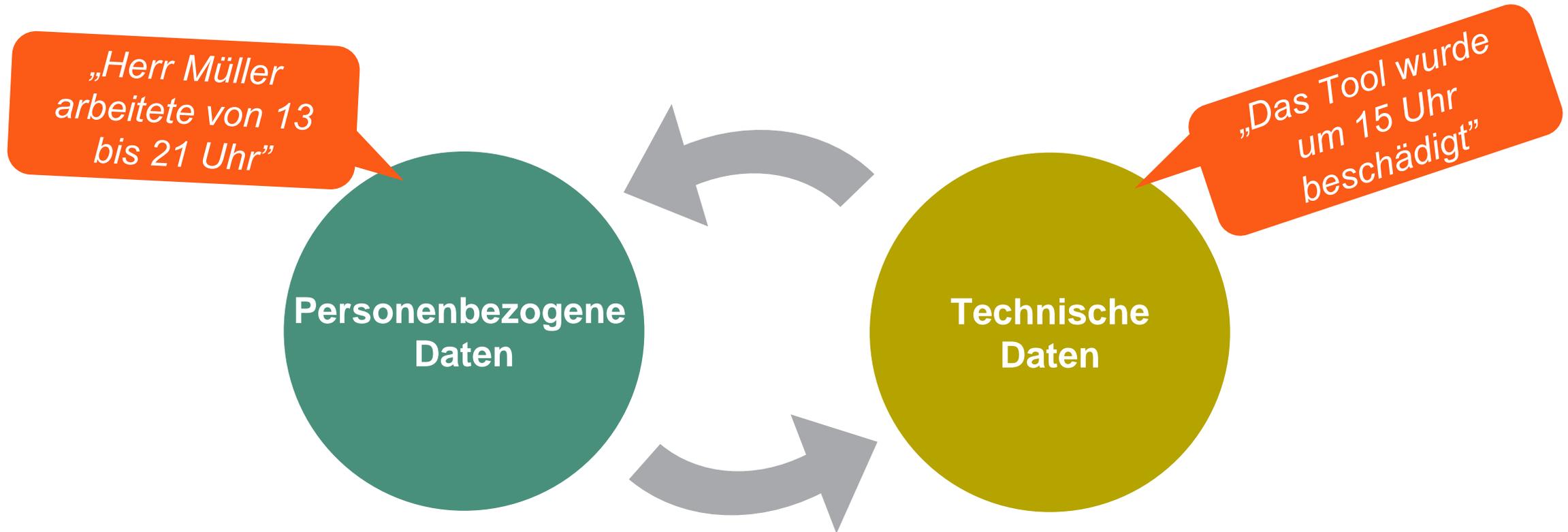
- Mangels gesetzlicher Vorschriften sind vertragliche Regelungen notwendig
- Das ist eine Chance: Der Spielraum ermöglicht eine weitgehende Flexibilität
- **Vorsicht:** Verkaufte Maschinen sind Eigentum des Kunden. Ein Zugriff ohne vertragliche Zustimmung kann sogar strafbar sein (Data Act enthält explizite Regelung)



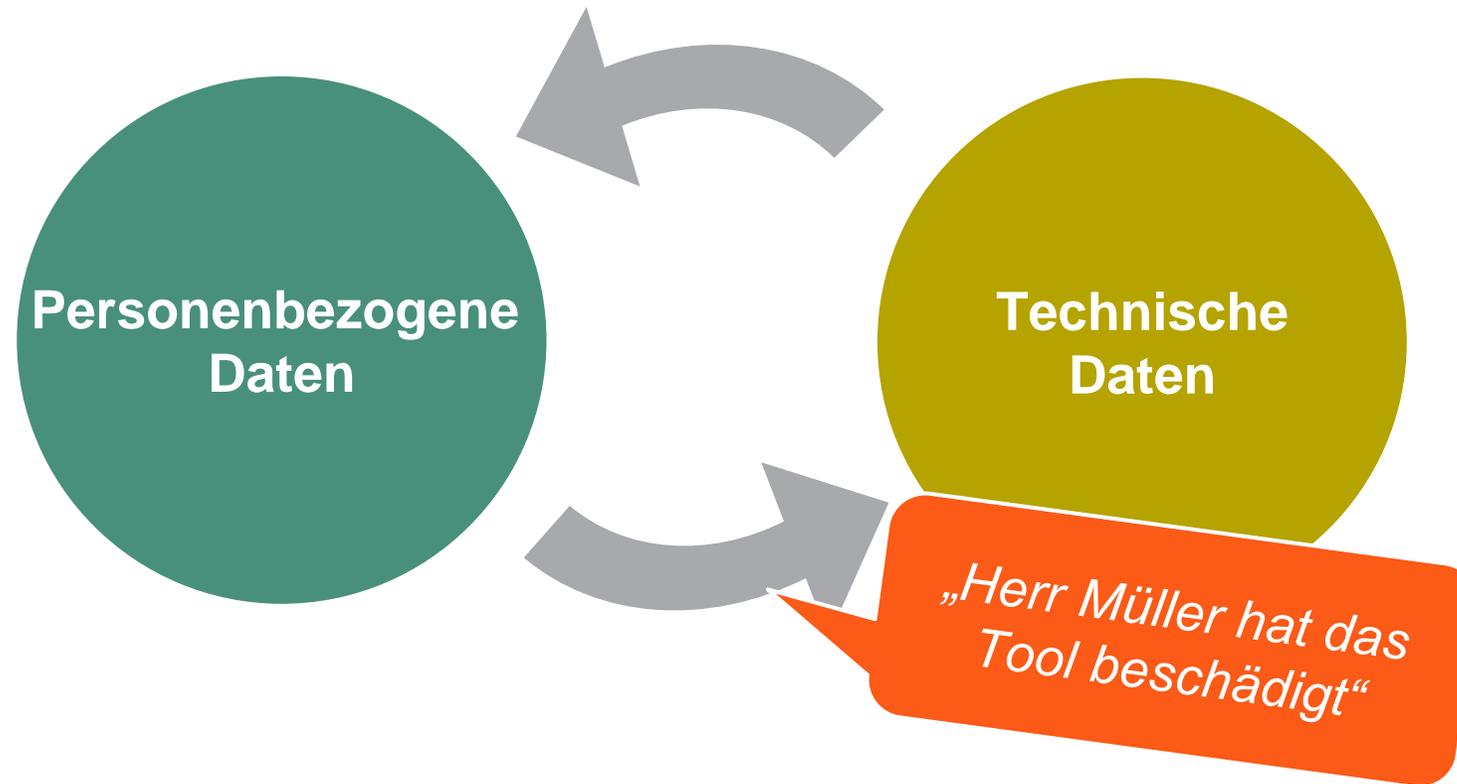
Betrifft das Datenschutzrecht alle Daten?



Die Verknüpfung mit Zusatzinformationen ist entscheidend ...



... und führt zum Personenbezug der Daten



Kann man der DSGVO entkommen?

„...sofern irgendjemand die Person identifizieren kann“

„... sofern der Verantwortliche die Person hinreichend identifizieren kann“

Absolute Theorie

„... rechtliche Mittel verfügbar, die es erlauben, die Person bestimmen zu lassen ...“
(EuGH, Urt. v. 19.10.2016)

Relative Theorie

Es ist schwierig der DSGVO zu enkommen, aber Datenschutz ist selten der kritischste Punkt für Projekte im Maschinenbau

Abschluss einer Vereinbarung gem. Art. 26 bzw. 28 DSGVO (als Teil der AGB)

Problem der Unterauftragsverarbeitung thematisieren

Anonymisierung vor Weiterverwendung der Daten

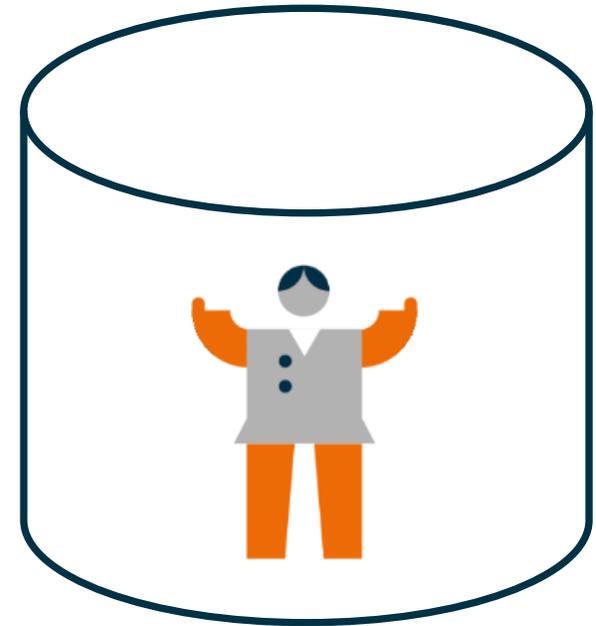
Einbindung des Betriebsrates oder sonstiger Mitarbeitervertretungen

Implementierung geeigneter Datensicherheitsmaßnahmen

Entwicklung einer leicht umsetzbaren Auditierungsroutine

Erstellung einer Datenschutzerklärung

Berücksichtigung von Speicherorten und Drittlandsdatentransfers



Contents

- 01 Komplexität durch das multipolare Geschäftsmodell

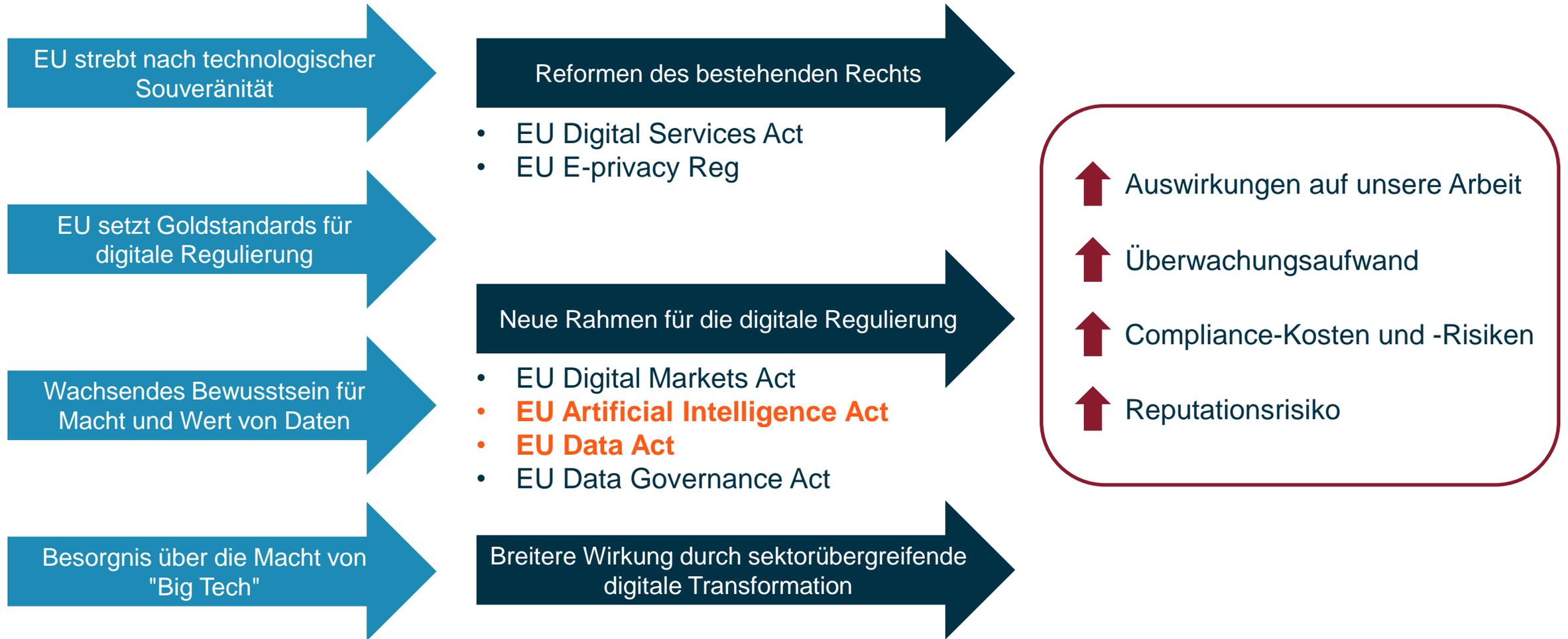
- 02 Komplexität durch bestehende Regulierung

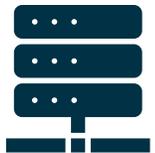
- 03 Komplexität durch kommende Regulierung**

- 04 Management der Komplexität in Verträgen und Prozessen



Sektorübergreifender digitaler Wandel: Wachsender Einfluss digitaler Regulierung





“The Data Act will be an important step in unlocking a wealth of industrial data in Europe, benefiting businesses, consumers, public services and society as a whole.

It will form the cornerstone of a strong, innovative and sovereign European digital economy.”

- Thierry Breton, Commissioner for the European Internal Market



Worum geht es beim Data Act?



Hersteller von IoT-Produkten bieten Funktionen, die Daten generieren, diese Daten bestellt der Hersteller meist



Der Wert dieser Daten soll für die europäische Wirtschaft realisiert werden



Hindernisse beim Zugriff auf diese Daten sollen abgebaut werden, wobei die Anreize zur Generierung von Daten erhalten bleiben sollen

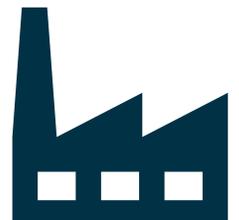


Recht auf Zugang zu und Weitergabe der Daten für Nutzer



Zentrale Verpflichtungen bezüglich des Zugangs zu Daten bei vernetzten Produkten (1/2)

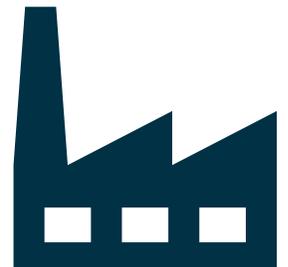
- i. Gestalten Sie das vernetzte Produkt so, dass die von dem vernetzten Produkt standardmäßig erzeugten **Daten für den Nutzer leicht und gegebenenfalls direkt zugänglich** sind.
- ii. Ist ein direkter Zugang nicht möglich, muss der Dateninhaber die von dem vernetzten Produkt erzeugten Daten dem Nutzer (kostenlos, fortlaufend und in Echtzeit) zur Verfügung stellen:
 - a. **Bereitstellung eines einfachen Anfragevorgangs auf elektronischem Wege für die Nutzer.**
 - b. **Geschäftsgeheimnisse müssen nur offengelegt werden, wenn alle Maßnahmen zur Wahrung der Vertraulichkeit eingehalten werden (Dateninhaber und Nutzer können entsprechende Maßnahmen vereinbaren).**
- iii. Auf Anfrage des Nutzers, stellen Sie die von dem vernetzten Produkt erzeugten Daten einem Dritten zur Verfügung (z.B. einem anderen Unternehmen oder einer öffentlichen Einrichtung, mit bestimmten Ausnahmen für Anbieter von zentralen Plattformen):
 - a. **Der Dateninhaber kann von dem Dritten verlangen, dass er bestimmten Bedingungen für die Bereitstellung der Daten zustimmt; die Bedingungen müssen fair, angemessen und dürfen nicht diskriminierend sein.**
 - b. **Geschäftsgeheimnisse dürfen grundsätzlich nicht an Dritte weitergegeben werden.**
 - c. **Der Dateninhaber kann ggf. eine Ausgleichszahlung von einem Dritten verlangen.**



Zentrale Verpflichtungen bezüglich des Zugangs zu Daten bei vernetzten Produkten (2/2)

- iv. Machen Sie **transparent, welche Daten zugänglich** sind, wie auf sie zugegriffen werden kann, wie der Hersteller die Daten verwendet und wer der Dateninhaber ist, bevor Sie einen Vertrag mit dem Nutzer über das vernetzte Produkt abschließen.
- v. Der **Dateninhaber** kann alle nicht personenbezogenen Daten, die von dem angeschlossenen Produkt erzeugt werden, nur auf der Grundlage einer **vertraglichen Vereinbarung mit dem Nutzer** verwenden.
- vi. Der Dateninhaber kann personenbezogene Daten, die von dem vernetzten Produkt generiert werden, nur mit einer Rechtsgrundlage gemäß der DSGVO (Erwägungsgrund 24) verwenden; der vorgeschlagene Data Act schafft keine Rechtsgrundlage.
- vii. Der Dateninhaber stellt die von dem vernetzten Produkt erzeugten Daten im Falle von außergewöhnlicher Notwendigkeit (z.B. Pandemie, öffentlicher Notstand, Beseitigung der Folgen eines öffentlichen Notstands) öffentlichen Stellen zur Verfügung.

Kleinst- und Kleinunternehmen sind von diesen Verpflichtungen ausgenommen.



KI breitet sich mit jeder Definition mehr aus

Hochrangige Expertengruppe für KI

„Systeme der künstlichen Intelligenz (KI-Systeme) sind (...) Softwaresysteme (...), die in Bezug auf ein komplexes Ziel (...) handeln, indem sie ihre **Umgebung durch Datenerfassung wahrnehmen**, die gesammelten (...) **Daten interpretieren, Schlussfolgerungen daraus ziehen** (...) und über das **bestmögliche Handeln zur Erreichung des (...) Ziels** entscheiden. KI-Systeme (...) sind (...) in der Lage, die Auswirkungen ihrer (...) Handlungen (...) zu analysieren **und ihr Verhalten (...) anzupassen.**“

DSK (Positionspapier TOM KI)

„Ein KI-System beinhaltet in der Regel mindestens eine KI-Komponente. Unter einer KI-Komponente wird eine **Abbildungsvorschrift** verstanden, die durch Verfahren **maschinellen Lernens** gebildet wurde.“

Beispiele maschinellen Lernens im Positionspapier:

- Lineare Regression
- K-Means Clustering
- Klassifikations- und Regressionsbaum-verfahren (CART)

AI-Act

„(...) (KI-System) [bezeichnet] eine Software, die mit einer (...) der in Anhang I aufgeführten Techniken (...) entwickelt worden ist und im Hinblick auf (...) Ziele (...), Ergebnisse wie (...) Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen(...)“

Techniken in Anhang I:

- Konzepte des maschinellen Lernens (einschl. Deep Learning)
- Logik- und wissensgestützte Konzepte
- Statistische Ansätze

Artificial Intelligence Act – Ein risikobasierter Ansatz



Artificial Intelligence Act – Pflichten bei Hochrisiko-KI Systemen

Für die Hochrisiko-KI besteht ein umfassender Katalog an Pflichten und Anforderungen (Art. 8-51 AI-Act), z.B.:

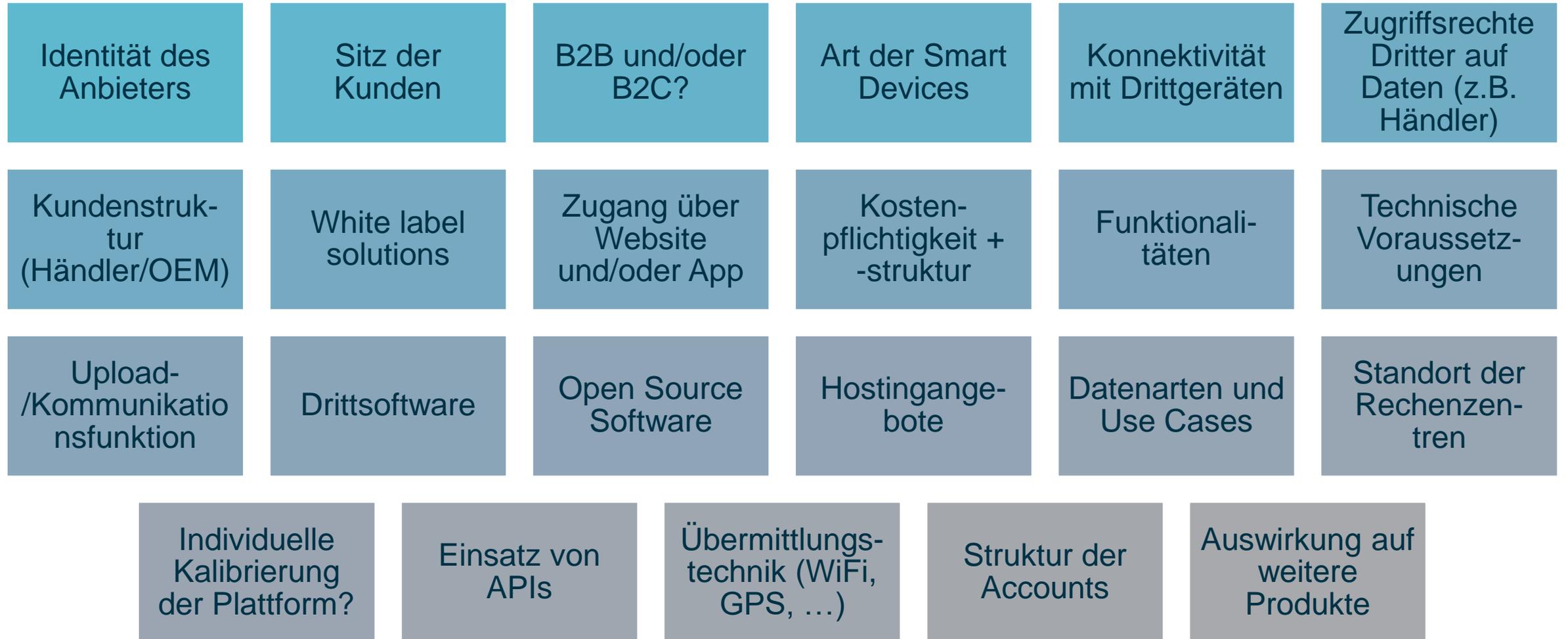
- Einrichtung eines Risikomanagementsystems
- Technische Dokumentation und Aufzeichnung von Ereignissen
- Transparenz- und Informationspflichten
- Konzeption des KI-Systems mit der Möglichkeit menschlicher Aufsicht
- Konzeption des KI-Systems mit einem angemessenem Maß an Genauigkeit, Robustheit und Cybersicherheit
- Rollenspezifische Pflichten, wie Qualitätsmanagementpflichten für Anbieter von Hochrisiko-KI
- Zertifizierungspflichten

Contents

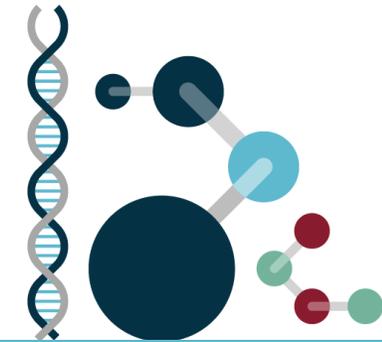
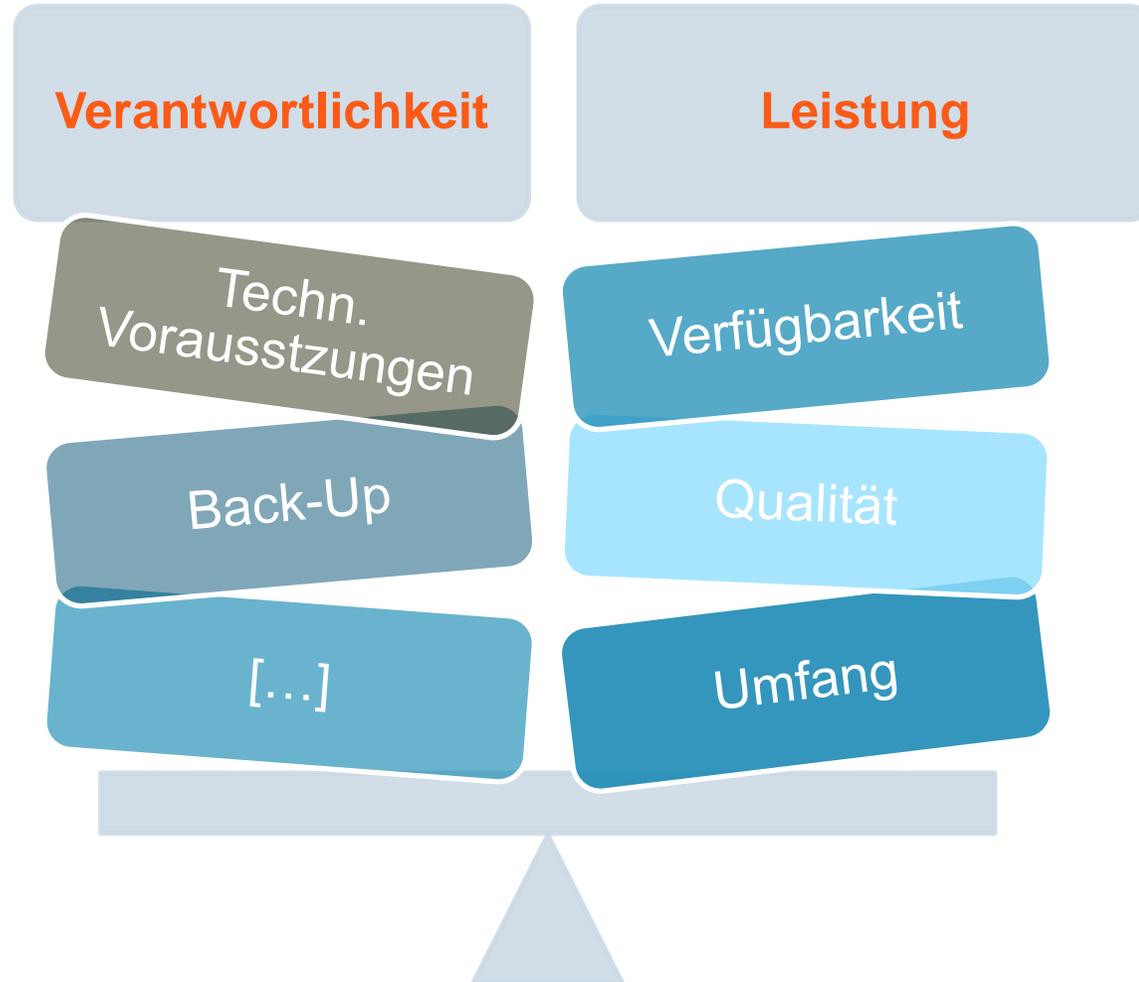
- 01 Komplexität durch das multipolare Geschäftsmodell
 - 02 Komplexität durch bestehende Regulierung
 - 03 Komplexität durch kommende Regulierung
 - 04 Management der Komplexität in Verträgen und Prozessen**
-



Let's talk business – Wichtige Fragen im Zusammenhang mit IoT

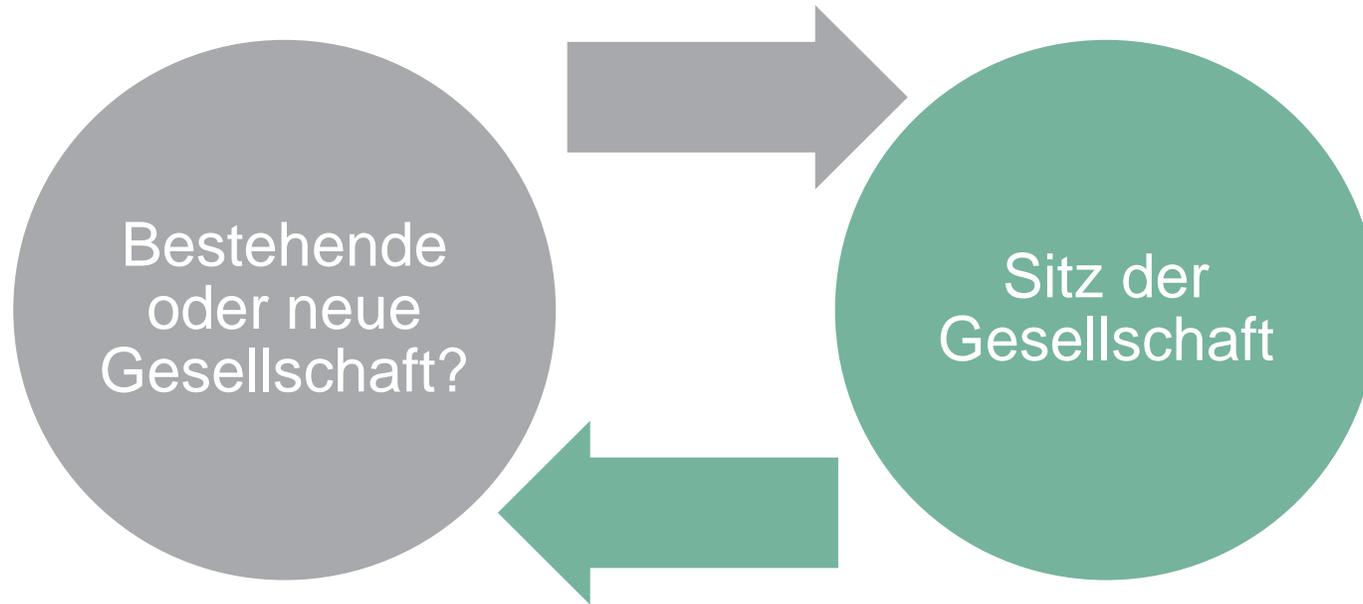


Leistungsbeschreibung



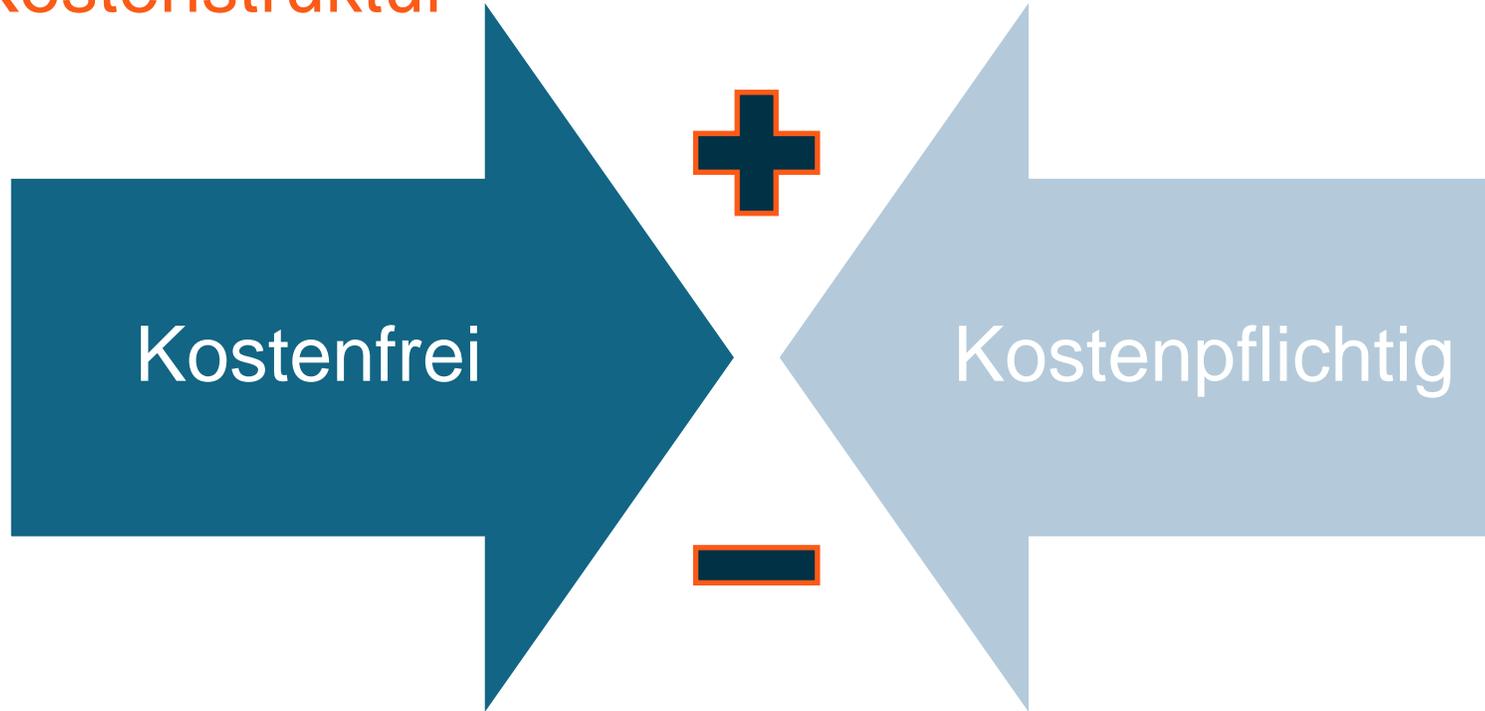
Die konkreten Leistungen müssen klar geregelt werden

Identität des Anbieters



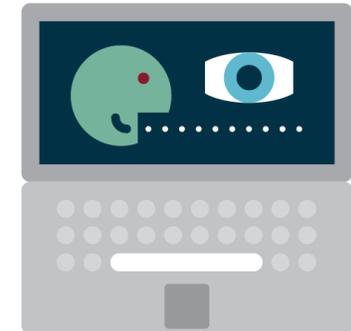
Die Identität des Anbieters muss für die Vertrags-gestaltung feststehen (insbesondere in internationalen Konstellationen)

Kostenstruktur



Größerer **Spielraum** im Vertragsrecht und bei den möglichen technischen und vertraglichen Änderungen

- **Lizenzregelungen:** Mengen und Bezüge (Kopplung an Nutzer/Geräte)
- **Kostenstrukturen:** Abo- / Subscription-Modell?



Die Kostenstruktur beeinflusst die Zulässigkeit der AGB

Datenarten und Use Cases der Nutzung



Fazit

Digitale Geschäftsmodelle im Maschinenbau führen zu **komplexen Vertragsstrukturen**

Datenschutz muss immer durchdacht werden

Der **Wert der Daten** muss vertraglich abgesichert werden (abhängig vom Datenfluss)

Künftige Regulierung wird digitale Geschäftsmodelle **massiv beeinflussen**

In der **Vertragsgestaltung** ist die Komplexität beliebig steigerbar.

