DSGVO, ISO27001 und KI-VO

Traum oder Albtraum?

23.10.2024 it-sa

caralegal

Agenda

1. “Datenschutz und KI sind nicht miteinander vereinbar.”

2. KI-VO trifft auf internationale Datenregulierungen:
   Ein Puzzle oder ein Meisterwerk?

caralegal

1.

“Datenschutz und KI

sind nicht miteinander vereinbar.”

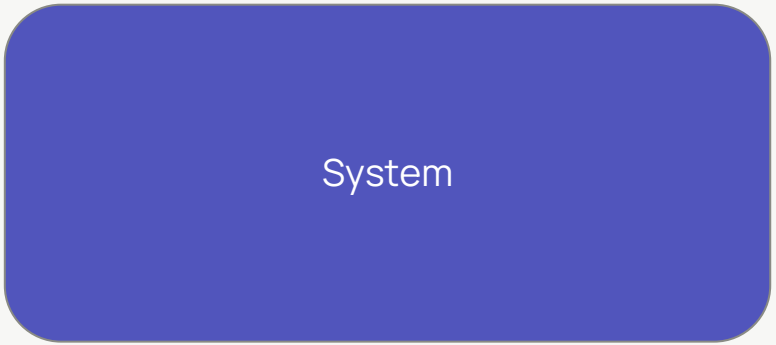
Die Definition der KI laut KI-VO

“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”

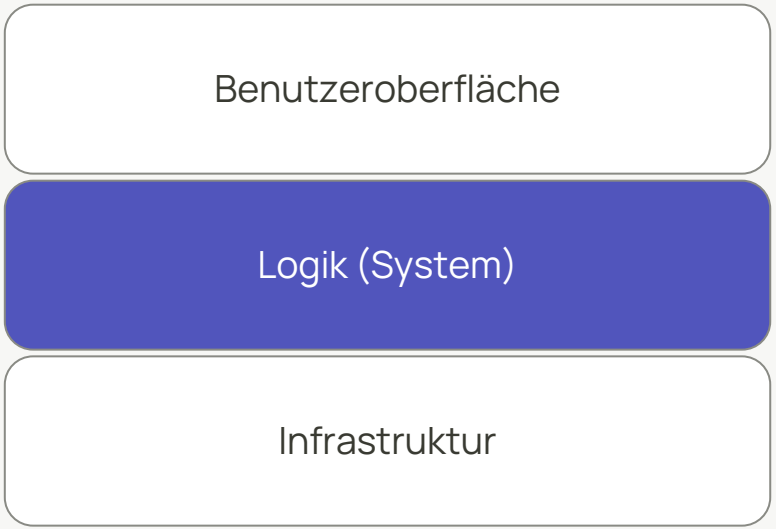
1. Autonom

2. Adaptiv

3. System


System


Anwendung
Infrastruktur

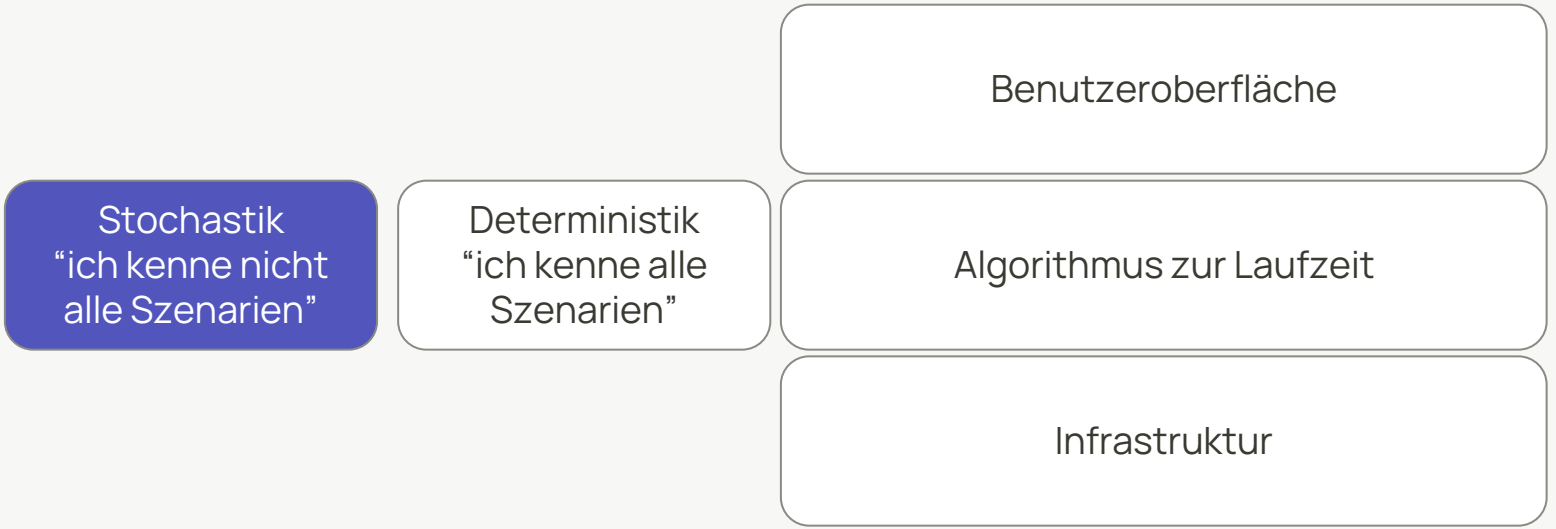

Benutzeroberfläche
Logik (System)
Infrastruktur

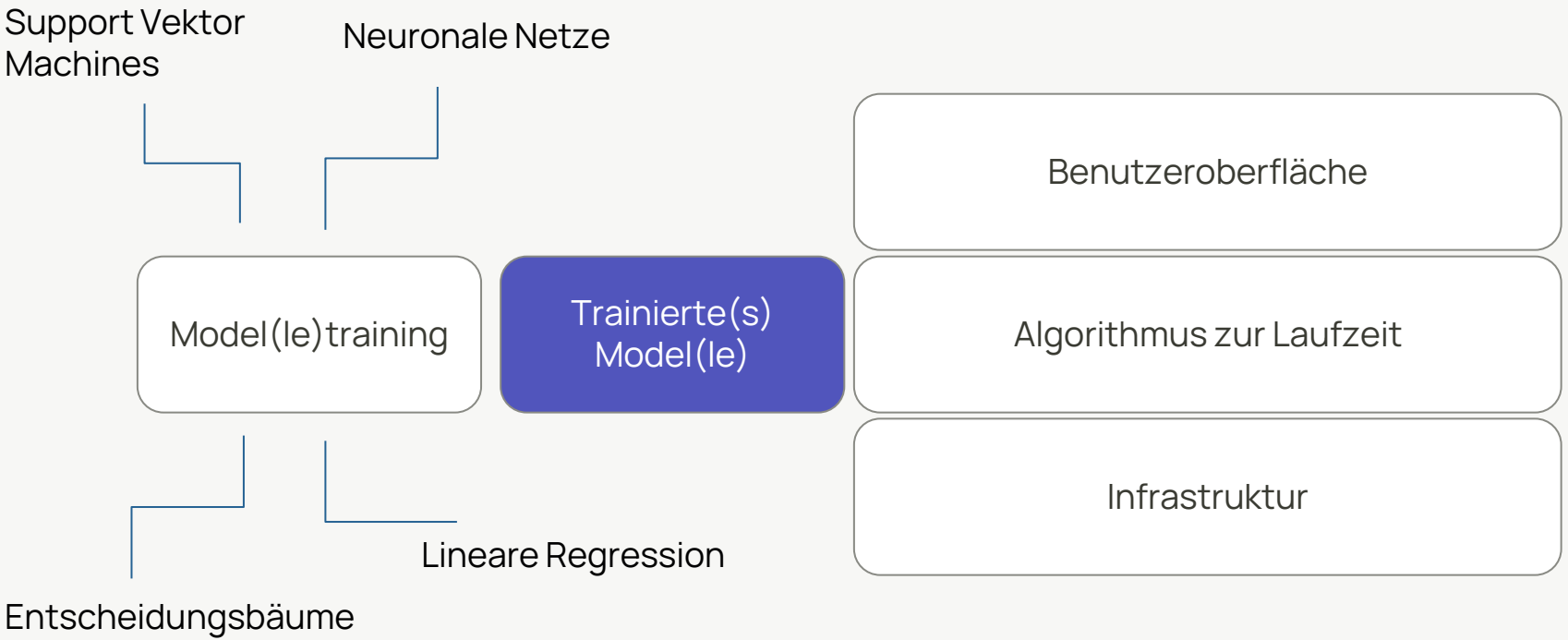
Entwicklung des Algorithmus

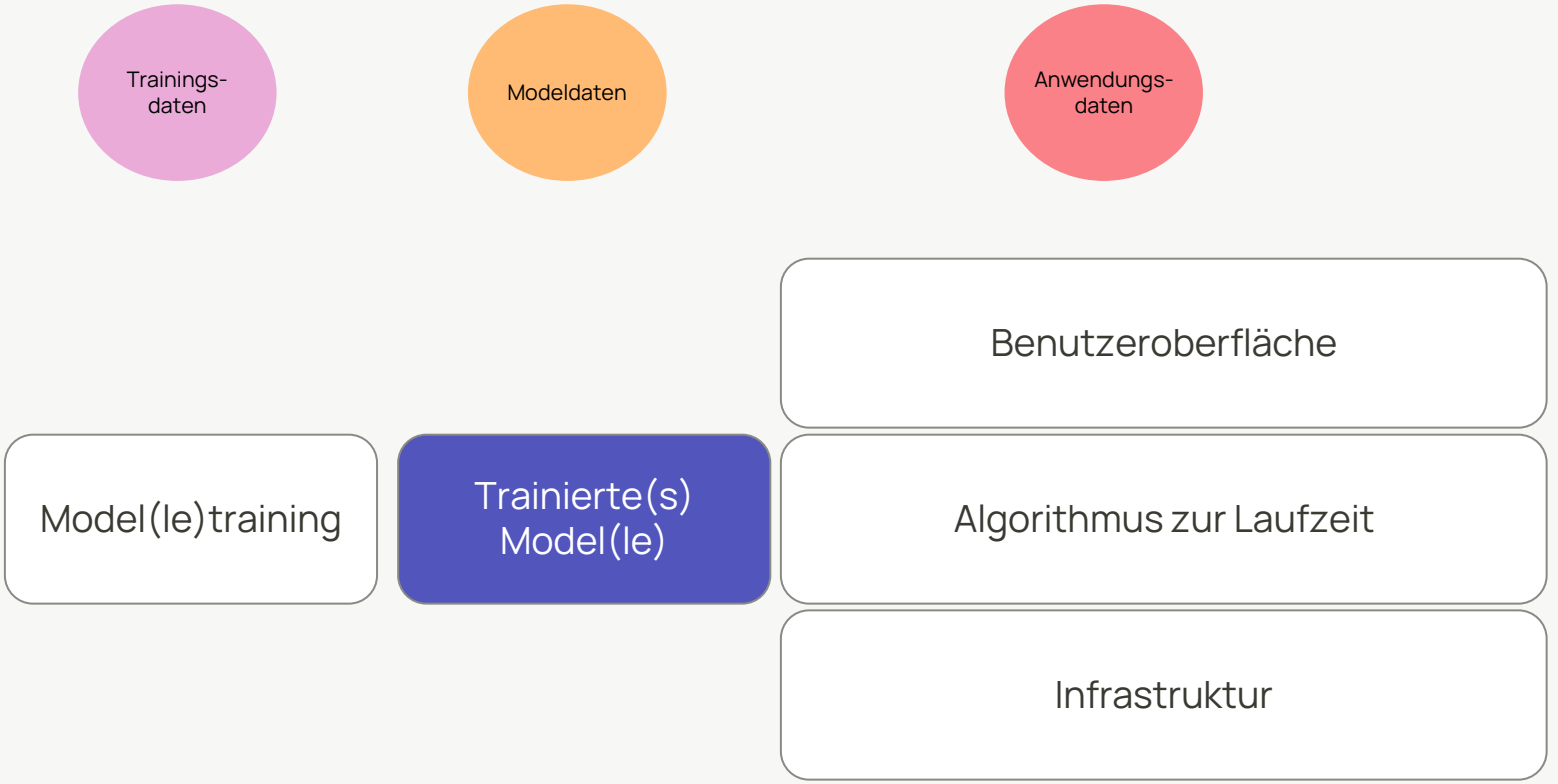
Benutzeroberfläche

Algorithmus zur Laufzeit

Infrastruktur


Stochastik
“ich kenne nicht alle Szenarien”
Deterministik
“ich kenne alle Szenarien”
Benutzeroberfläche
Algorithmus zur Laufzeit
Infrastruktur


Support Vektor Machines
Neuronale Netze
Model(le)training
Trainierte(s) Model(le)
Benutzeroberfläche
Algorithmus zur Laufzeit
Infrastruktur
Lineare Regression
Entscheidungsbäume


Trainings-
daten
Modeldaten
Anwendungs-
daten
Benutzeroberfläche
Model(le)training
Trainierte(s)
Model(le)
Algorithmus zur Laufzeit
Infrastruktur

Trainings-daten

Können personenbezogene Daten enthalten.

- Text
- Bilder
- Sprache

Modeldaten

Sind Zahlen.

- Gewichtungen
- Hyperparameter
- Architektur-beschreibung

Anwendungs-daten

Können pers. bez. Daten bei In- und Output enthalten.

- Text
- Bilder
- Sprache

Trainings-daten

Modeldaten

Anwendungs-daten

Können personenbezogene Daten enthalten.

- Text
- Bilder
- Sprache

Sind Zahlen.

- Gewichtungen
- Hyperparameter
- Architektur-beschreibung

Können pers. bez. Daten bei In- und Output enthalten.

- Text
- Bilder
- Sprache

Trainieren

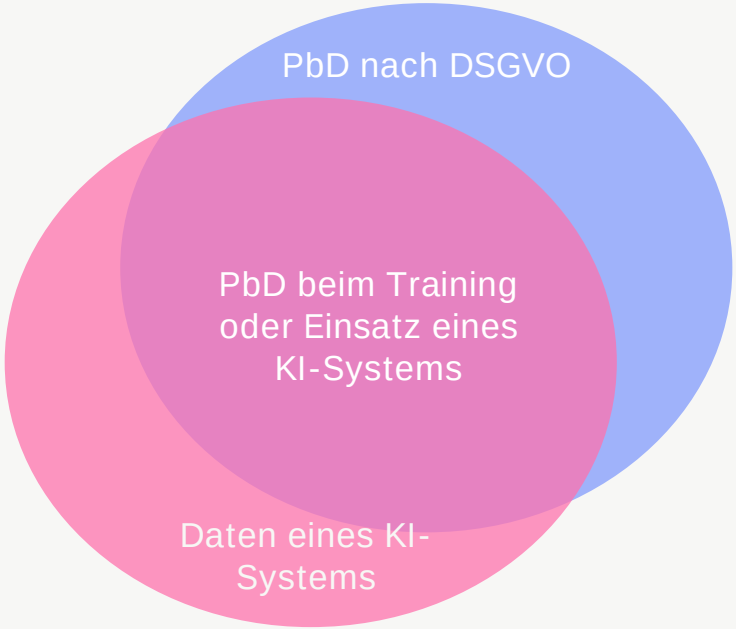
Keine Verarbeitungs-tätigkeit*

Anwenden

*https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf

KI-VO lässt DSGVO im Grundsatz unberührt

1. Beide Verordnungen gelten **nebeneinander**
2. **Schnittstellen** ergeben sich dort, wo KI-System pbD verarbeitet:
   - ➢ Auf der Entwicklungsebene können pbD zum Training oder zum Testen des KI-Systems verarbeitet
   - ➢ Beim Einsatz des KI-Systems können pbD verarbeitet
3. Alleinige Anwendung des AI-Act nur bei nicht-pbD, z. B. Training mit synthetischen Daten, Wetterdaten, Antibakterienforschung, Finanzielle Forecasts u. v. m.



Parallelität der Anforderungen: KI-VO & DSGVO

KI-VO	Datengovernance, Art. 10 Abs. 3	Aufzeichnungspflichten, Art. 12	Genauigkeit, Robustheit und Cybersicherheit, Art. 15	Grundrechte-**Folgenabschätzung** Art. 27
Pflichten nach KI-VO	Trainings-, Validierungs- und **Testdatensätze** müssen relevant, repräsentativ, fehlerfrei und vollständig sein "beabsichtigten Zweck so weit wie möglich fehlerfrei und vollständig sein"	Vollständige Protokollierung von Vorgängen und Ereignissen während der gesamten Lebensdauer (inkl. Rückverfolgbarkeit)	Angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit	u.a. Beschreibung der Verfahren, vorhergesehenen Zweck u. Einsatzbereich; potenziell betroffener Personenkreis & deren Schadensrisiken
DSGVO	Richtigkeit, Art. 5 Abs. 1 lit. d; **Integrität und Vertraulichkeit**, Art. 5 Abs. 1 lit. f	Rechenschaftspflicht, Art. 5 Abs. 2; Datenminimierung, Art. 5 Abs. 1 lit. c	TOM, Art. 32; Privacy by Design, Art. 25 Abs. 1	DSFA, Art. 35; Zweckbindung, Art. 5
Wechselwirkungen zwischen KI-VO und DSGVO	KI-VO + DSGVO **ergänzen** sich. Aufgrund der unterschiedlichen Regelungsrichtung müssen beide VO beachtet werden	Konflikt möglich. Bei der Protokollierung nach KI-VO ist auf Datensparsamkeit zu achten. Nur notwendige pbD protokollieren. **Datenadäquanz**.	KI-VO erweitert Schutzziele / Gewährleistungsziele der DSGVO; Sicherheitsmaßnahmen nach KI-VO sind daher, um Maßnahmen nach DSGVO zu erweitern	DSFA + GRFA können unter gewissen Voraussetzungen gemeinsam durchgeführt werden; DSFA soll als Annex bei Veröffentlichung der GRFA beigefügt werden

caralegal

2.

KI-VO trifft auf globale Datenregulierungen

Ein Puzzle oder ein Meisterwerk?

Frage: Wie viele Listen von ‘Verzeichnissen’ gibt es bei Ihnen?

A

1

Dank konsistenter Dokumentation

B

3

Bisher VVT, BCM und ab jetzt noch die Verzeichnisse für KI Anwendungsfälle

C

>10

Weil ist wichtig

Datenregulatorische compliance als Ergebnis der Integration von DSGVO, KI-VO, NIS2, Dora, APPI…

Verarbeitungstätigkeit dokumentieren

Art. 30 DS-GVO

Führung der Dokumentation

Art. 11 KI-VO

!?

Dokumentierte Information

ISO 27001 Anforderung 7.5

Governance und Organisation

Art. 5 DORA

Datenregulatorische compliance als Ergebnis der Integration von DSGVO, KI-VO, NIS2, Dora, APPI...

Verarbeitungstätigkeit dokumentieren

Art. 30 DS-GVO

!?

Führung der Dokumentation

Art. 11 KI-VO

Dokumentierte Information

ISO 27001 Anforderung 7.5

!?

Governance und Organisation

Art. 5 DORA

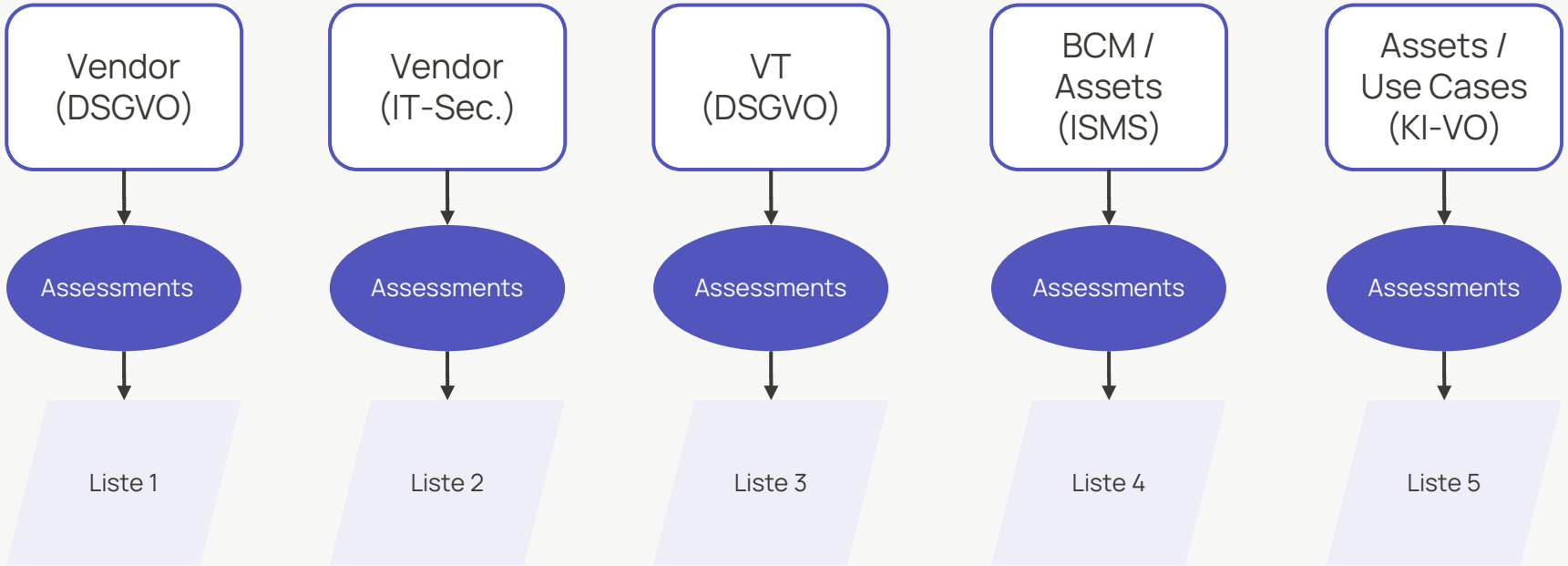
Contents of disclosure

§1798.110 CCPA

Specification of the Purpose of Utilization

Art. 15 APPI

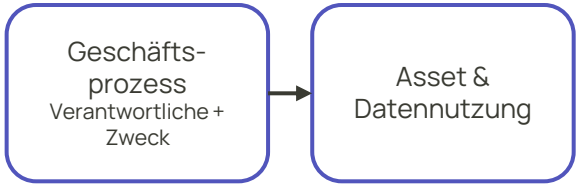
Möglichkeit 1: (Risk-)Assessments für jeden Bereich



Möglichkeit 2

Vermeidung von Doppelarbeit

Financial Forecast



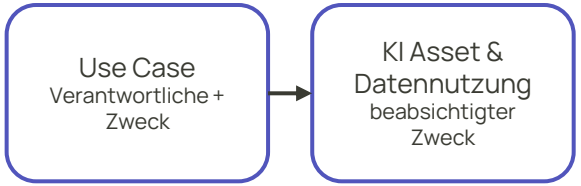
Data Responsibility

Oder Leichter: Keine Doppelarbeit

Dank One Flow.

KI basierter Sales Forecast

Financial Forecast



Data Responsibility

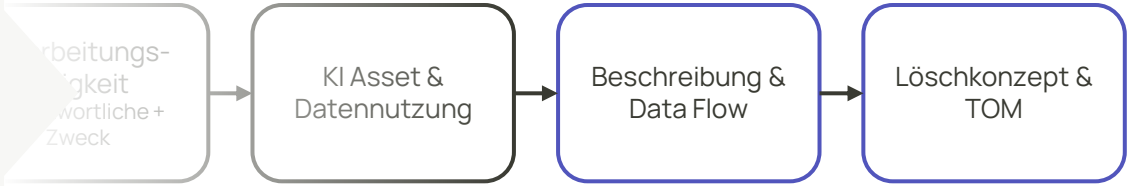
Oder Leichter: Keine Doppelarbeit

Dank One Flow.

Darstellung der Top-Seller

KI basierter Sales Forecast

Financial Forecast



Data Responsibility

Oder Leichter: Keine Doppelarbeit

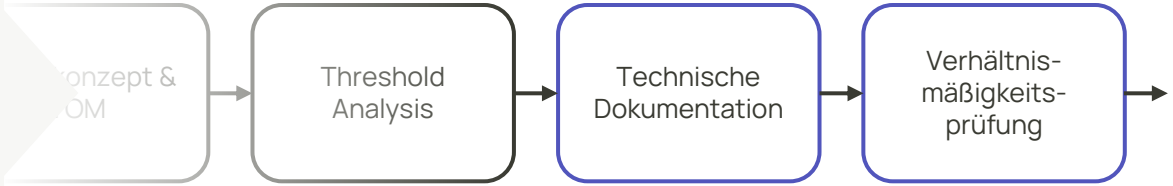
Dank One Flow.

Auto. Einstufung des Bonus nach Leistung und Gesundheit

Darstellung der Top-Seller

KI basierter Sales Forecast

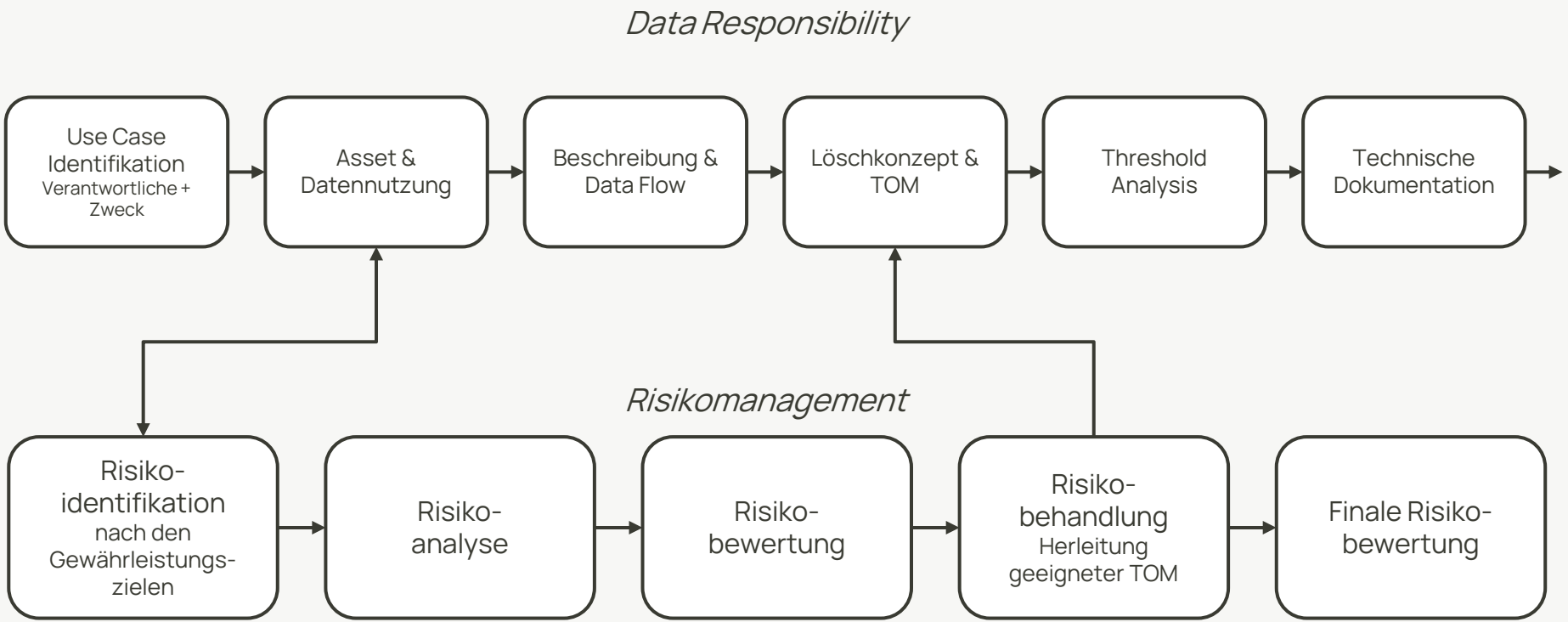
Financial Forecast



Data Responsibility

*https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_278/BGBLA_2018_II_278.pdfsig

Oder leichter: Keine Doppelarbeit dank One Flow.



Unique One-Flow

DSGVO	KI-VO
NIS2	DORA
DPDPA	CCPA
APPI	LGPD

Single Source of Truth

Datenschutz

IT-Security

AI-Governance

Fachbereich

Der AI-Act als Erfolgsfaktor

1. Datenschutz und KI sind ~~nicht~~ miteinander vereinbar.

2. KI-VO trifft auf internationale Datenregulierungen: Ein Puzzle oder ein Meisterwerk?

Ihr persönlicher Kontakt

We make the legal way the lighter way

www.caralegal.eu

Björn Möller

Geschäftsführer & CEO

bjoern.moeller@caralegal.eu

caralegal