Vortragsreihe: AI Act umsetzen

Künstliche Intelligenz und Datenschutz in der Praxis (Teil 1: Grundlagen)

Wer steht heute (virtuell) vor Ihnen?

Andreas Sachs

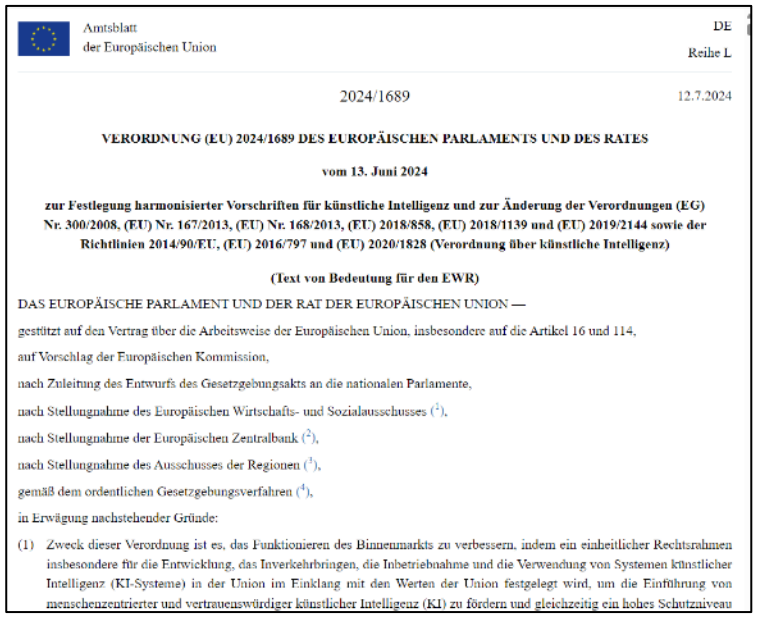
Informatiker

Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Vize-Präsident

Bereichsleiter Cybersicherheit und Technischer Datenschutz

KI-Beauftragter



Amtsblatt der Europäischen Union — DE — Reihe L

2024/1689 — 12.7.2024

VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Juni 2024

zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 16 und 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses [1],

nach Stellungnahme der Europäischen Zentralbank [2],

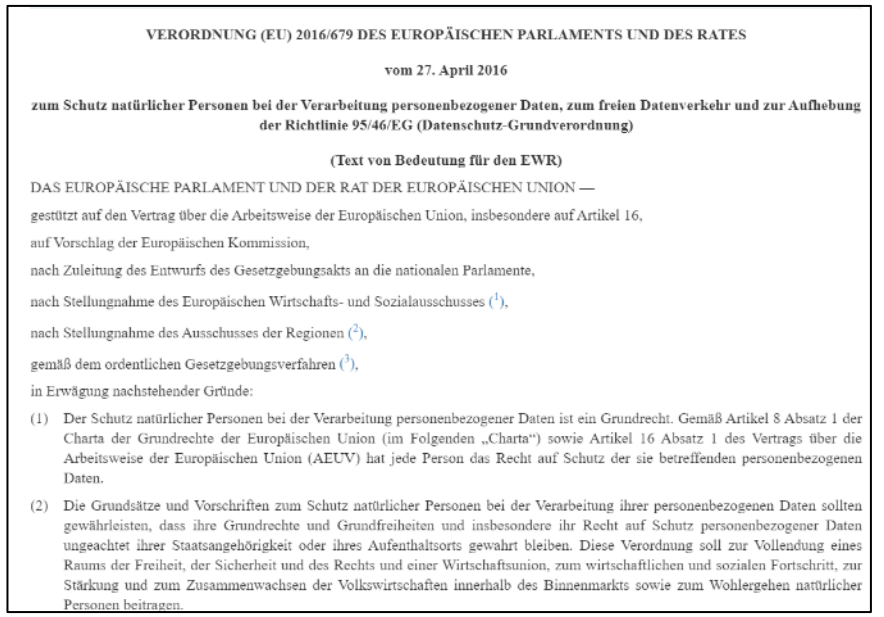
nach Stellungnahme des Ausschusses der Regionen [3],

gemäß dem ordentlichen Gesetzgebungsverfahren [4],

in Erwägung nachstehender Gründe:

(1) Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union im Einklang mit den Werten der Union festgelegt wird, um die Einführung von menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau

Die KI-Verordnung ist neu da und tritt ab 2025 schrittweise in Kraft



VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses [1],

nach Stellungnahme des Ausschusses der Regionen [2],

gemäß dem ordentlichen Gesetzgebungsverfahren [3],

in Erwägung nachstehender Gründe:

(1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

Die Datenschutzgrundverordnung feiert dieses Jahr den 6. Geburtstag

Worum geht es denn bei diesen Gesetzen überhaupt?

Beim Datenschutz:

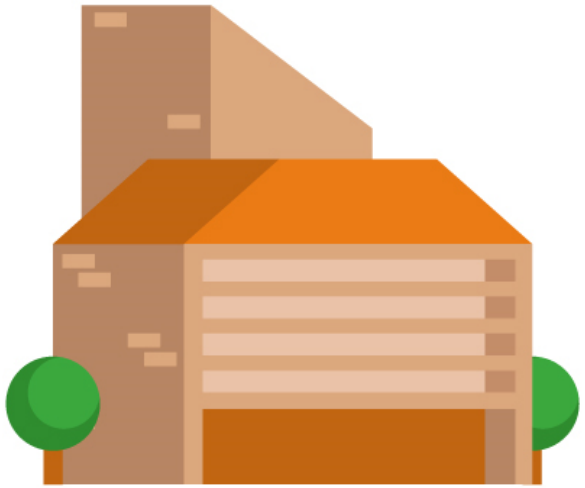
Es geht um Sie!

Und den **Schutz Ihrer Grundrechte** und Grundfreiheiten wenn Ihre personenbezogenen Daten verarbeitet werden

Stichworte:

- Grundrecht auf Datenschutz (Europäische Grundrechtecharta)
- Recht auf informationelle Selbstbestimmung

Beim Datenschutz:



Es geht aber auch um die Unternehmen

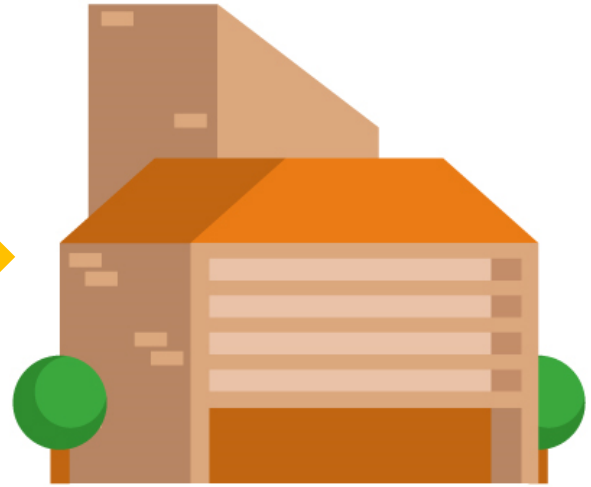
- Die **unternehmerische Freiheit** wird von der europäischen Grundrechtecharta ebenfalls anerkannt
- Gewährleistung des **freien Verkehrs personenbezogener Daten** zwischen den Mitgliedstaaten

Beim Datenschutz:

Betroffener

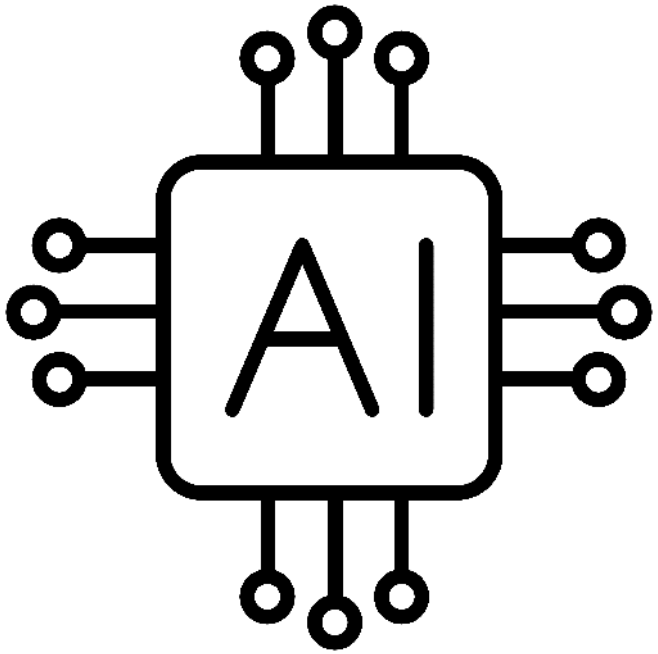
Ausgleich der Interessen

Datenschutzgrundverordnung
(DS-GVO)



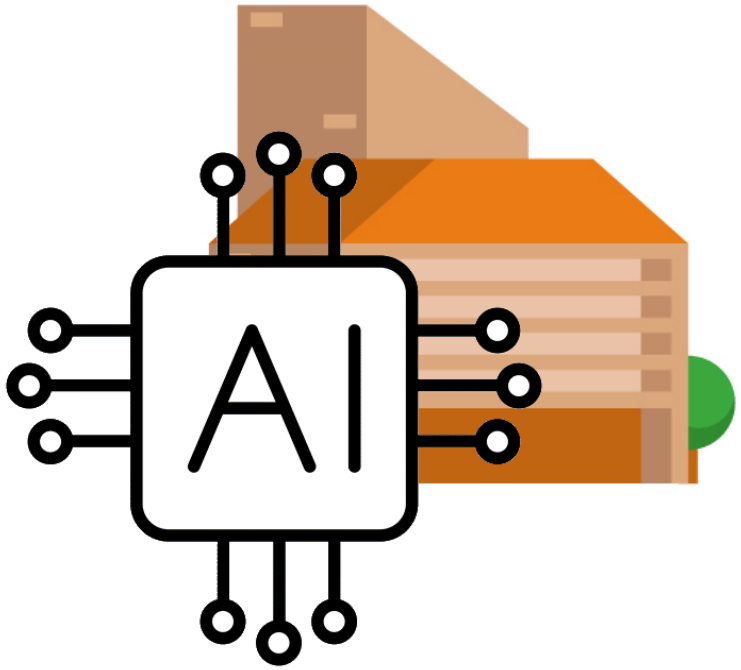
Verantwortlicher

In der KI-Verordnung:



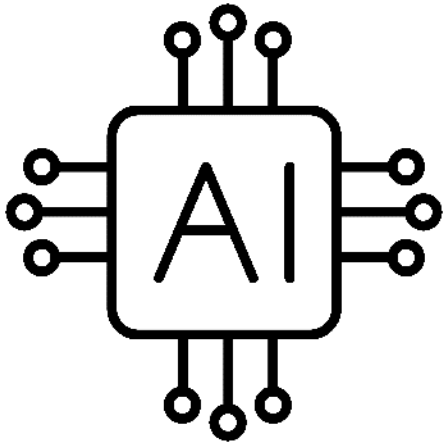
Regulierung von **Produkten** der Künstlichen Intelligenz (KI)

In der KI-Verordnung:



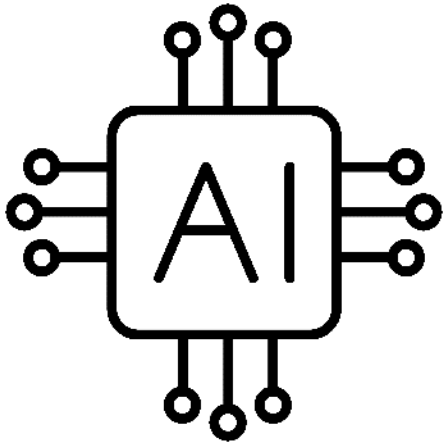
Aber auch:
Regulierung von **Betrieb** von Produkten der Künstlichen Intelligenz (KI) auf dem Markt (Marktüberwachung)

Ziel der KI-Verordnung:

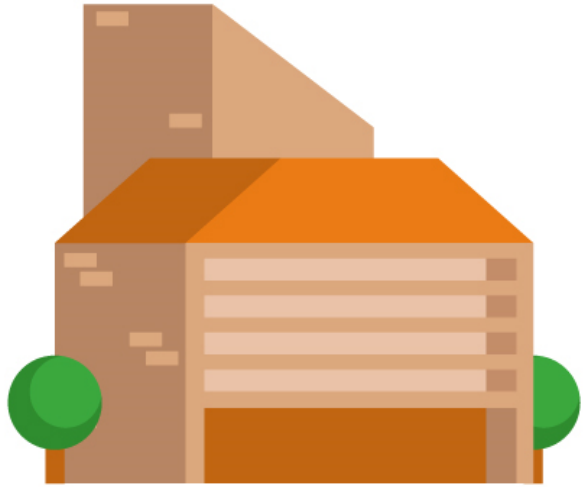


- Förderung einer auf den Menschen ausgerichteten **vertrauenswürdigen KI**
- **Hohes Schutzniveau** im Bereich Gesundheit, Sicherheit und Grundrechte

Ziel der KI-Verordnung:



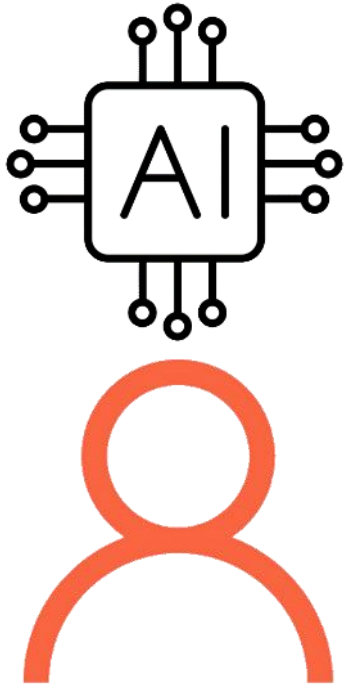
Unterstützung von Innovationen



Gemeinsamkeiten und Unterschiede

DS-GVO und KI-VO sollen den **Menschen schützen**

DS-GVO und KI-VO sollen den **freien Warenverkehr fördern**



DS-GVO reguliert die **Verarbeitung** personenbezogener Daten (mit KI-Produkten)

KI-VO reguliert die Markteinführung von **KI-Produkten**

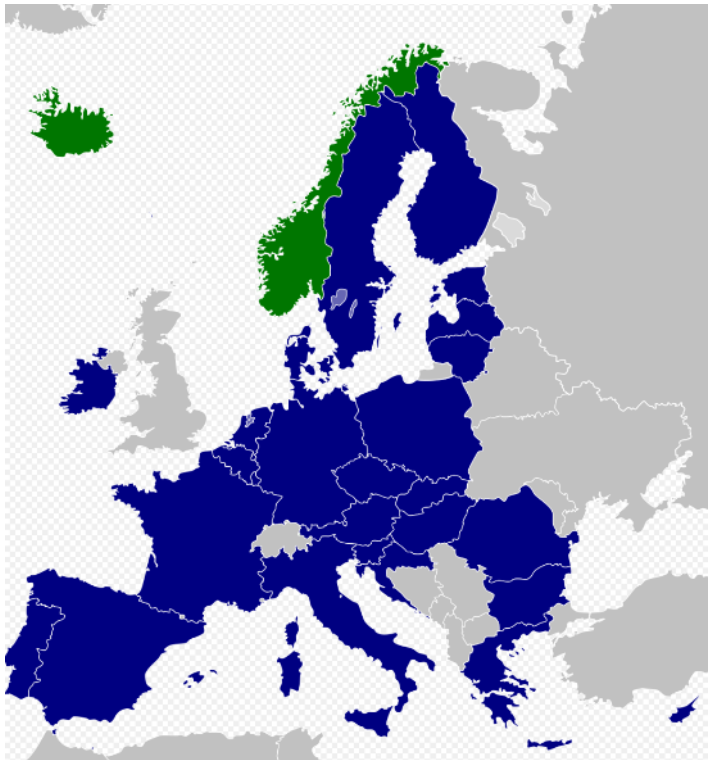
Jetzt schauen wir uns Datenschutz und KI genauer an

KI und Datenschutz in 8 Bausteinen

- Anwendungs-bereich
- Rollen und Verantwortlichkeiten
- Rechtsgrundlagen
- Privacy by Design
- Hochrisiko-KI
- Informations-pflichten
- Betroffenenrechte
- KI-as-a-Service

Anwendungsbereich

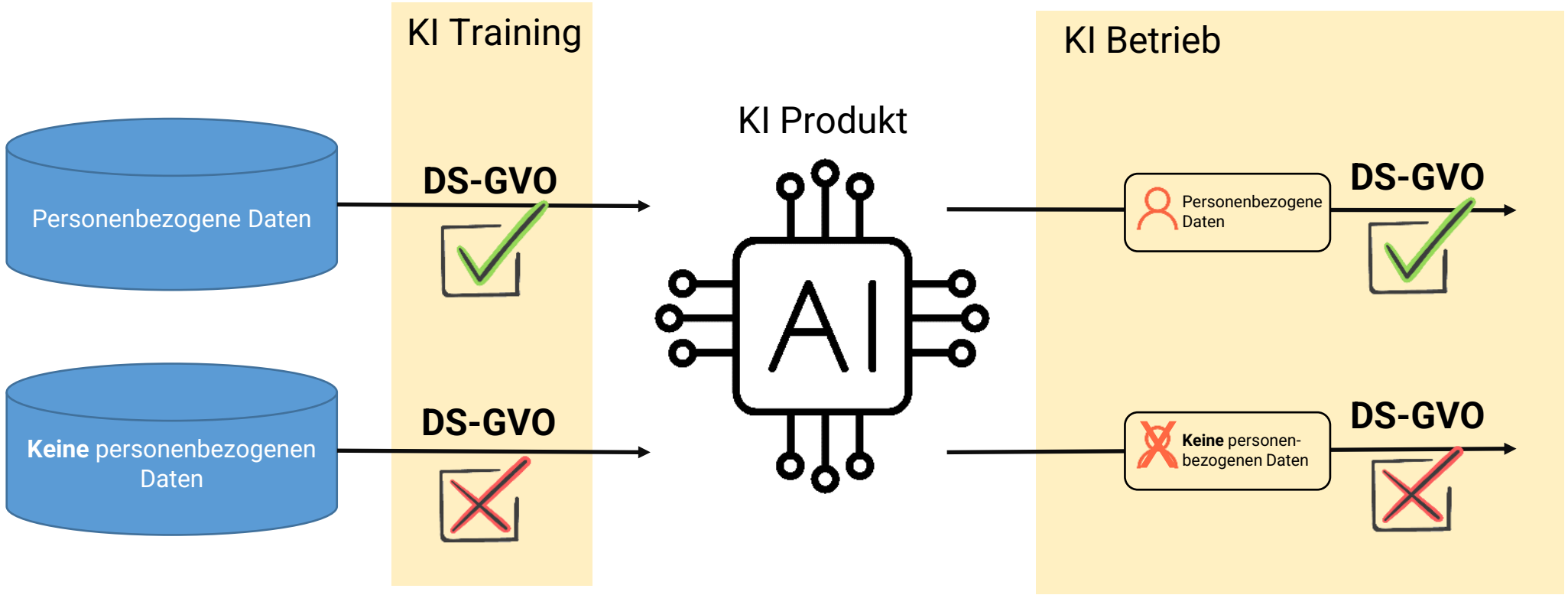
Anwendungsbereich: „*Gilt eine Regulierung für mich überhaupt?*“



Die DS-GVO und die KI-VO gilt für Unternehmen

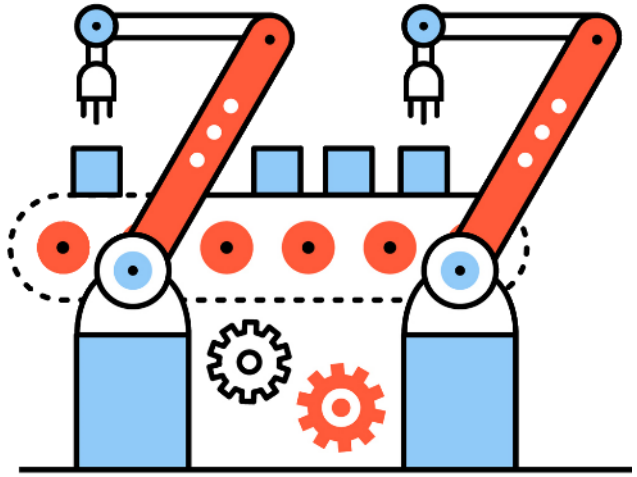
- mit Sitz in der EU/EWR
- die Waren und Dienstleistungen in EU/EWR anbieten

Anwendungsbereich: „*Gilt die Regulierung für mich überhaupt?*“



Anwendungsbereich: „*Gilt die Regulierung für mich überhaupt?*“

Beispiele:

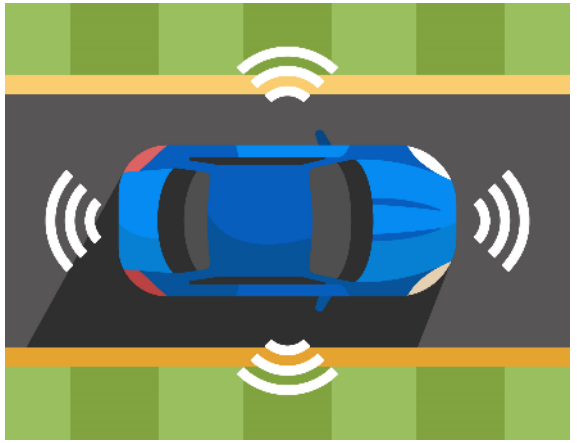


Industrielle Produktion mit KI

DS-GVO ✗

Chat-Bot zur Kundenkommunikation

DS-GVO ✓

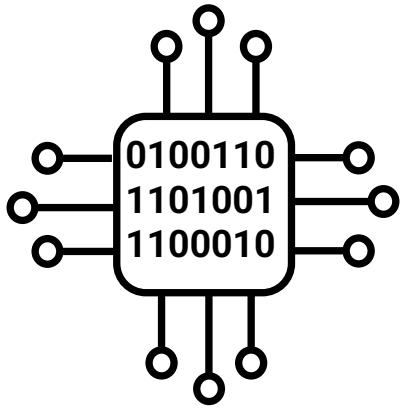


KI-Training beim automatisierten Fahren mit Echtdaten

DS-GVO ✓

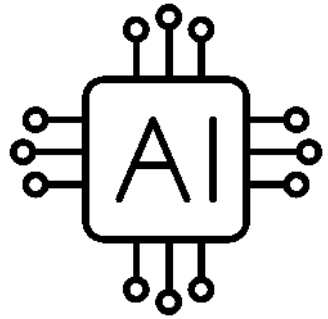
Einschub KI-VO: *„Gilt die Regulierung für mich überhaupt?“*

Technologie

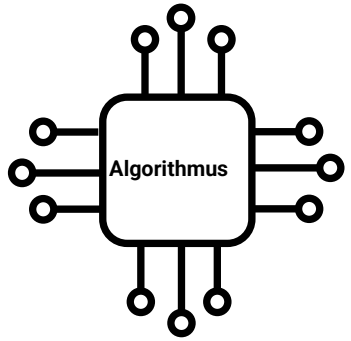


Checkliste

- ☐ Maschinengestützt?
- ☐ Anpassbar?
- ☐ Ziele ableitbar?
- ☐ Autonomiegrade?
- ☐ Beeinflussung Umgebung?



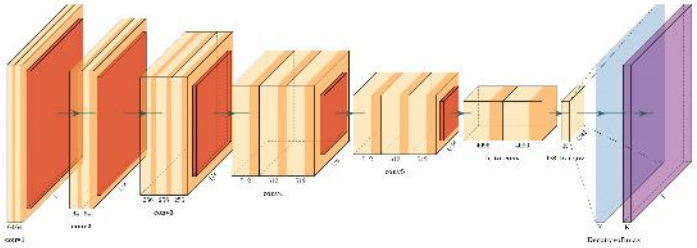
KI-VO ☑



KI-VO ☒

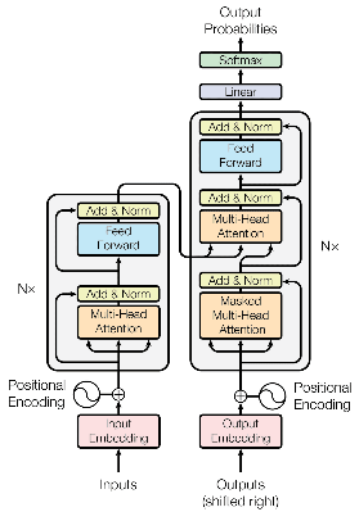
Einschub KI-VO: *„Gilt die Regulierung für mich überhaupt?“*

Beispiele (Technologie):



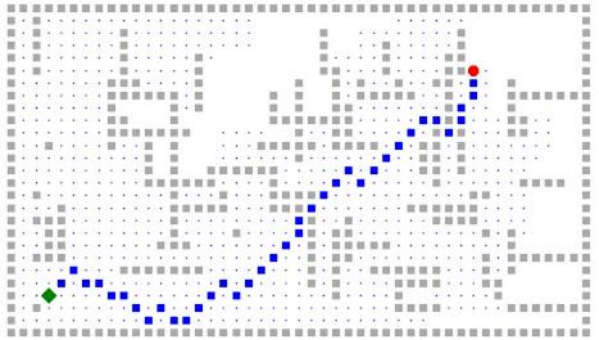
Tiefe Neuronale Netze

KI-System ✓



Große Sprachmodelle
mit Transformer-Architektur

KI-System ✓

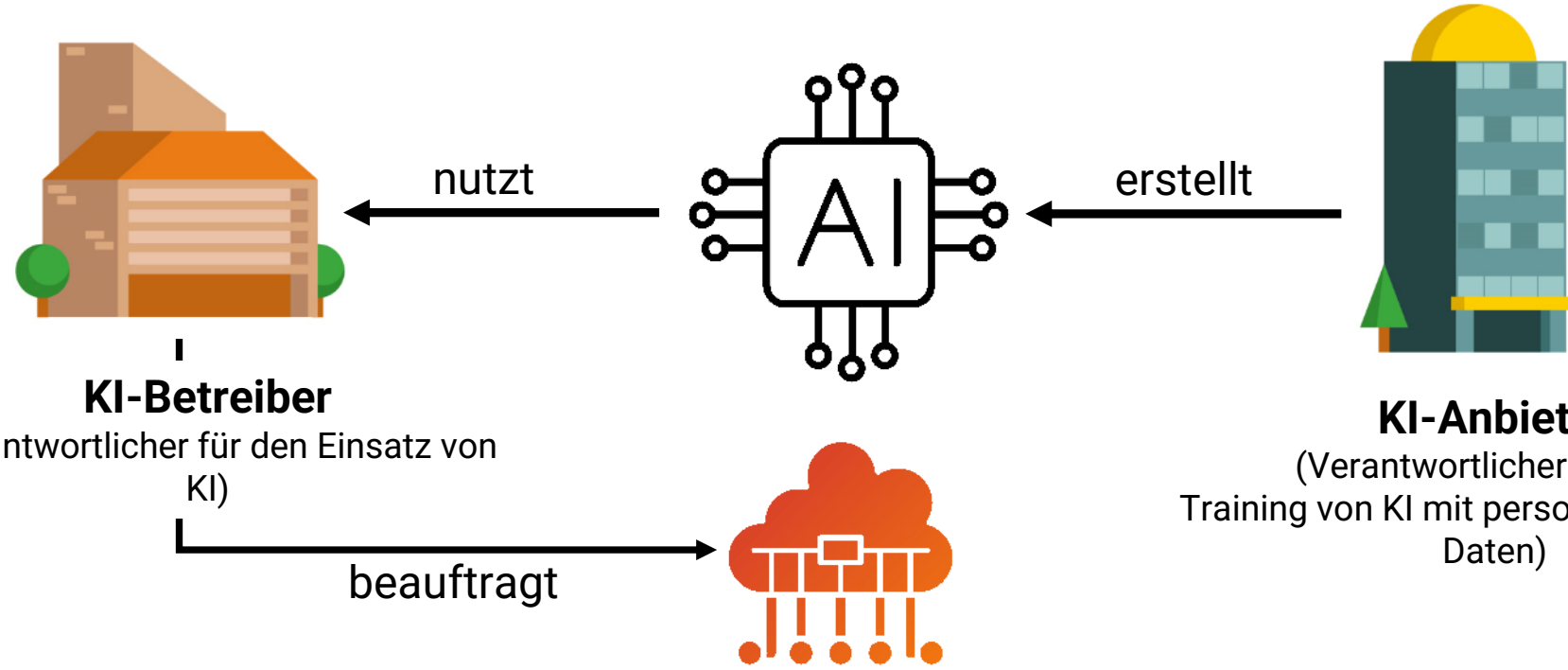


Cleverer
Suchalgorithmus

KI-System ✗

Rollen und Verantwortlichkeiten

DS-GVO: Rollen und Verantwortlichkeiten



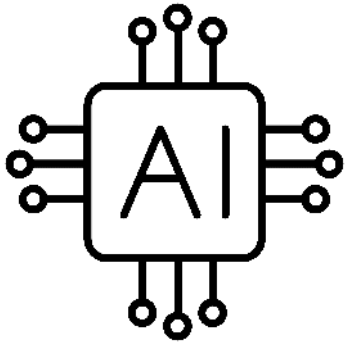
KI-Betreiber
(Verantwortlicher für den Einsatz von KI)

KI-Anbieter
(Verantwortlicher für das Training von KI mit personenbezogenen Daten)

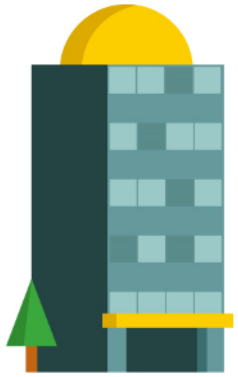
Dienstleister
(im Rahmen einer Auftragsverarbeitung)

KI-VO: Rollen und Verantwortlichkeiten

nutzt



erstellt



KI-Betreiber
(Verantwortlicher für den Einsatz von KI)

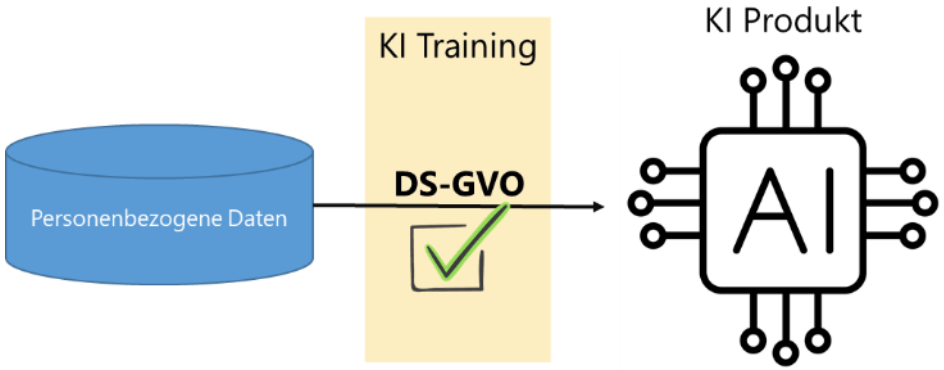
KI-Anbieter
(Verantwortlicher für die KI-Produkterstellung samt Markteinführung)

beauftragt

Dienstleister
(im Rahmen einer Auftragsverarbeitung)

Rechtsgrundlagen

DS-GVO: Rechtsgrundlagen für KI-Training

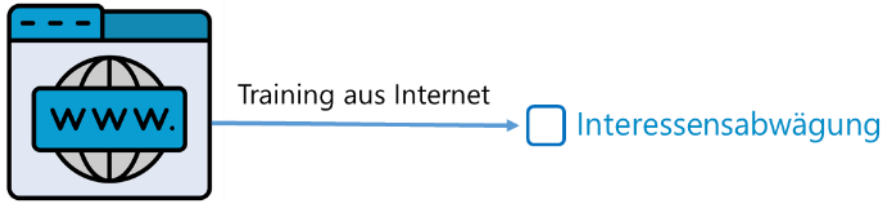


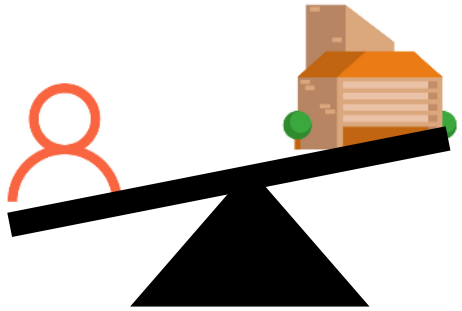
Training aus Internet

- **Zweck** der Verarbeitung: **KI-Training**
- Meist **sehr viele** (personenbezogene) **Daten erforderlich**
- Eine **hohe Datenqualität** ist unabdingbar

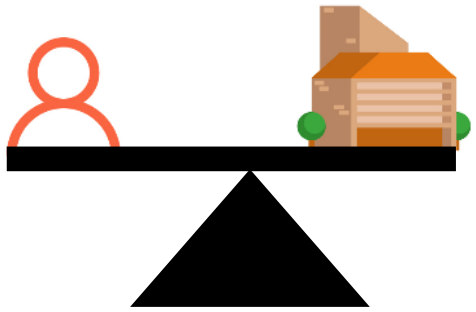
- Die **DS-GVO** bietet **mehrere Rechtsgrundlagen** an
  - ☐ Einwilligung
  - ☐ Vertrag
  - ☐ Gesetzliche Grundlage
  - ☐ Interessensabwägung (nicht-öffentliche Stellen)

DS-GVO: KI-Training aus Internet mit Interessensabwägung

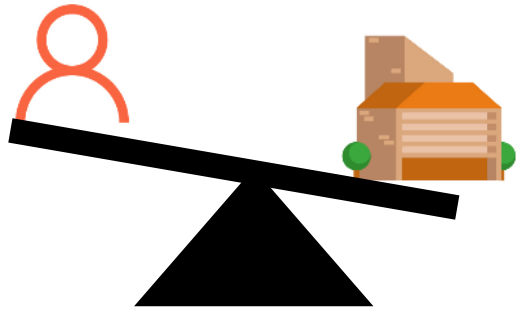




STOP KI-Training nicht zulässig (z.B. Daten von Kindern)



KI-Training zulässig



KI-Training zulässig

DS-GVO: KI-Training mit besonderen Arten personenbezogener Daten

Gesundheit

Ethnische Herkunft

Die Verarbeitung von Art.9 Daten ist untersagt

Die **DS-GVO** bietet **nur begrenzte Ausnahmen** an, z.B.

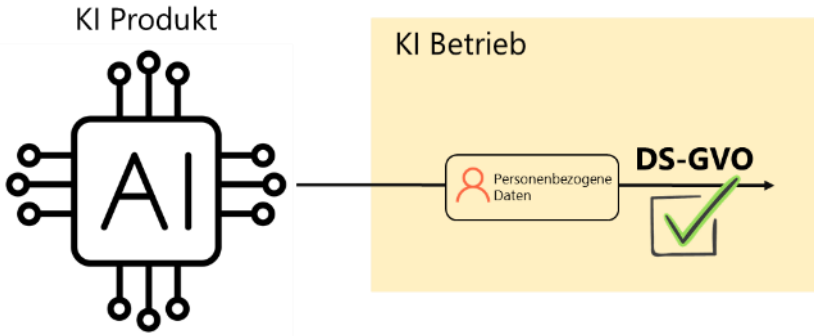
- ☐ Einwilligung
- ☐ Gesetzliche Grundlage

Sexuelle Orientierung

Biometrische Daten zur Identifizierung

- Wissenschaftliche Forschung
- Enge Zwecke + Gemeinwohlinteresse (bei Gesundheitseinrichtungen)
- Zwecke Gesundheit (zukünftig EHDS)

DS-GVO: Rechtsgrundlagen für KI-Betrieb



- Betreibersicht auf KI: ***„KI ist auch nur eine Software“***
- Die Rechtsgrundlage orientiert sich am **Zweck** der Verarbeitung
- Beispiele: Kundenkommunikation, Sichtung Bewerbungen, Betrugsprävention
- Ein KI-Produkt ist hier nur ein **Verarbeitungsmittel**
- Es können meist die **gleichen Rechtsgrundlagen** wie bei einer Verarbeitung **ohne KI** verwendet werden

Privacy by Design

DS-GVO: Datenschutz durch Technikgestaltung (Art. 25 DS-GVO)

DSK
DATENSCHUTZKONFERENZ

Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 06.11.2019

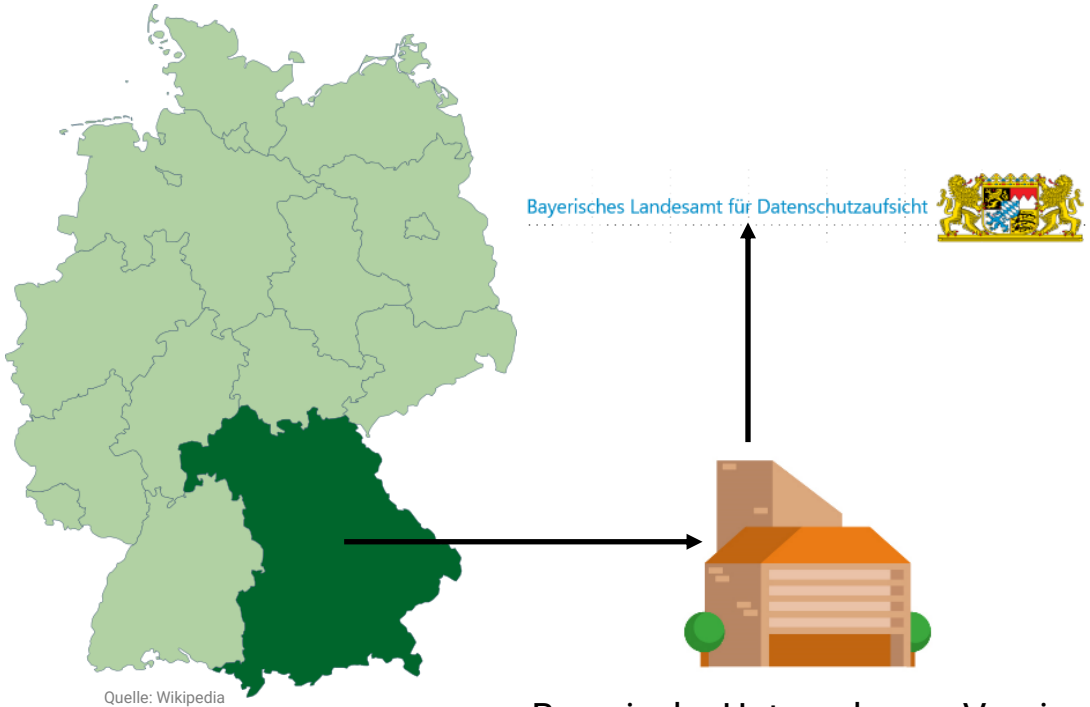
Stand: 06.11.2019

Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen

Abrufbar auch unter
https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

- Inhalt heute aus Zeitgründen nicht
- **Statt dessen** Anlass zu einer **wichtigen Frage**: Wie bekommen Unternehmen **Rechtssicherheit** von Seiten der **Datenschutzaufsichtsbehörden?**

DS-GVO: Dezentrale Aufsichtsbehörden, DSK und EDPB



Marktortprinzip der DS-GVO

- BayLDA ist die **einzige** Datenschutzaufsichtsbehörde für **alle bayerischen Unternehmen** (Arztpraxen, Vereine, Handwerk, Handel, Automotive, Gastgewerbe, Industrie, Startups,...)
- Ermöglicht die Aufsicht **unter Berücksichtigung regionaler Besonderheiten** (z.B. Sektoren, Unternehmensgröße, Vereinsdichte, Ehrenamt,...)
- Ermöglicht **direkte Beratung** (Sandbox-Prinzip)
- Ermöglicht **unkomplizierte Angebote für mehr Rechtssicherheit** (z.B. Checklisten, FAQs)

DS-GVO: Dezentrale Aufsichtsbehörden, DSK und EDPB

Quelle: Wikipedia

Manchmal braucht man **Rechtssicherheit von außerhalb Bayerns**

- **Dienstleistern** (als Auftragsverarbeiter) können **Kunden** in **anderen Bundesländern** oder **anderen europäischen Ländern** haben
- **Größere Konzerne** (Konzernholding) können **Konzerntöchter** in **anderen Bundesländern** oder **anderen europäischen Ländern** haben

DSK
DATENSCHUTZKONFERENZ

edpb
European Data Protection Board

Einbringen bayerischer regionaler Besonderheiten in der Datenschutzaufsicht

Bayerisches Landesamt für Datenschutzaufsicht

Dienstleister mit Hauptsitz in Bayern

Größere Konzerne mit Hauptsitz in Bayern und vielen Konzerntöchtern

DS-GVO: Informationen zu KI von Aufsichtsbehörden

Europäischer Datenschutzausschuss

www.edpb.europa.eu

Datenschutzkonferenz

www.datenschutzkonferenz-online.de

Bayerisches Landesamt für Datenschutzaufsicht

www.lda.bayern.de/ki

DS-GVO: Dezentrale Aufsichtsbehörden, DSK und EDPB


Quelle: Wikipedia

Fachgremien

edpb European Data Protection Board

DSK

Bayerisches Landesamt für Datenschutzaufsicht

Guidelines
Opinions

Orientierungshilfen
Anwendungshinweise

Checklisten
Informationen
Auslegungshilfen

Zielsetzung: Harmonisierung

Dienstleister

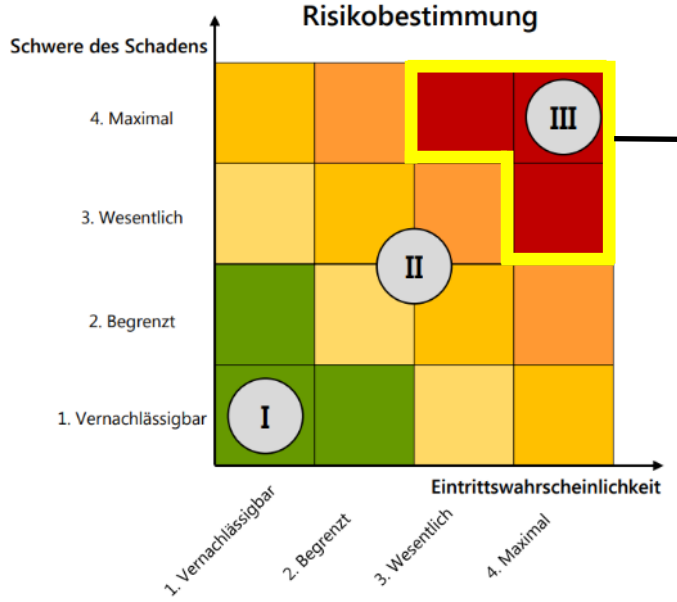
Größere Konzerne

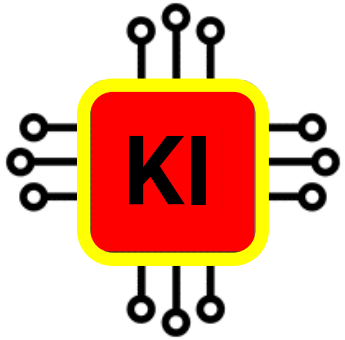
Bayerische Unternehmen, Vereine, Ärzte,...

Hochrisiko-KI

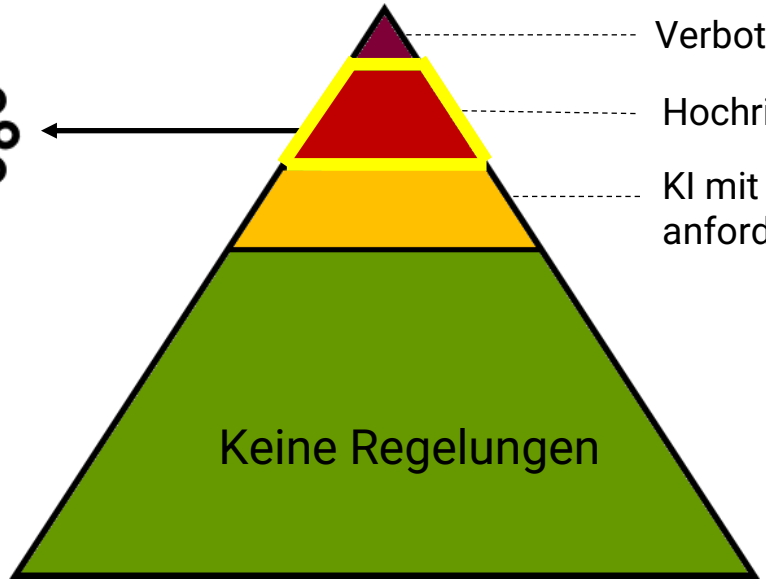
Hochrisiko-KI und Datenschutzfolgenabschätzung

DS-GVO



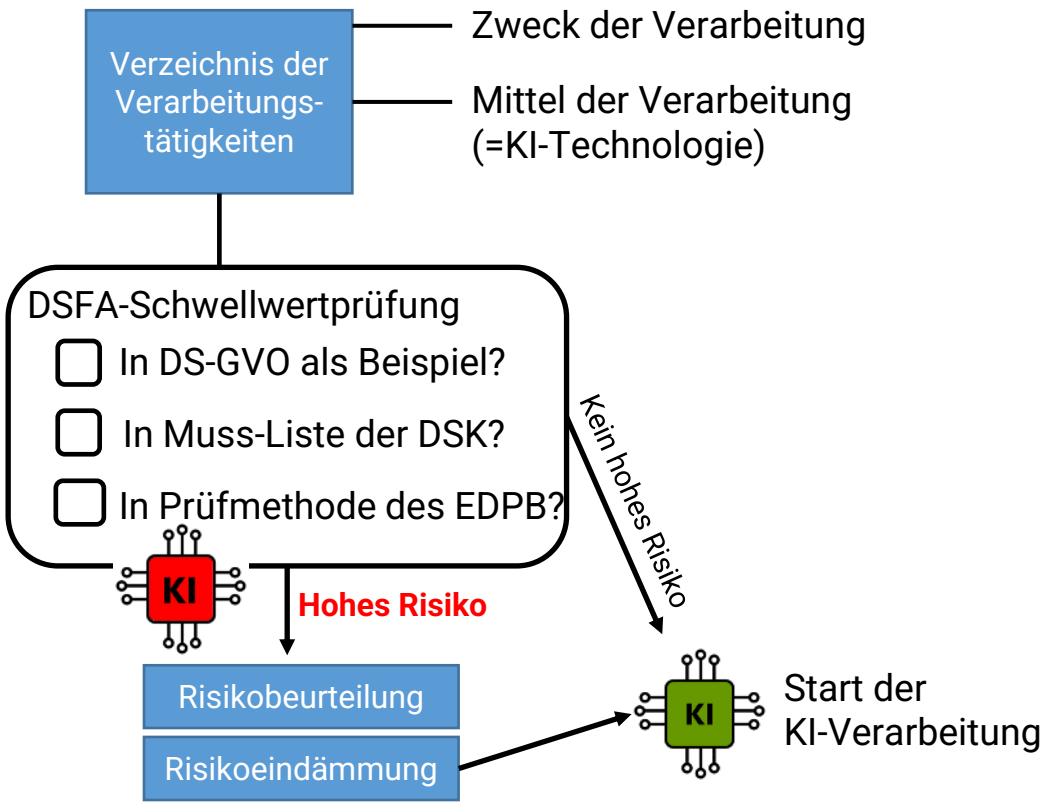


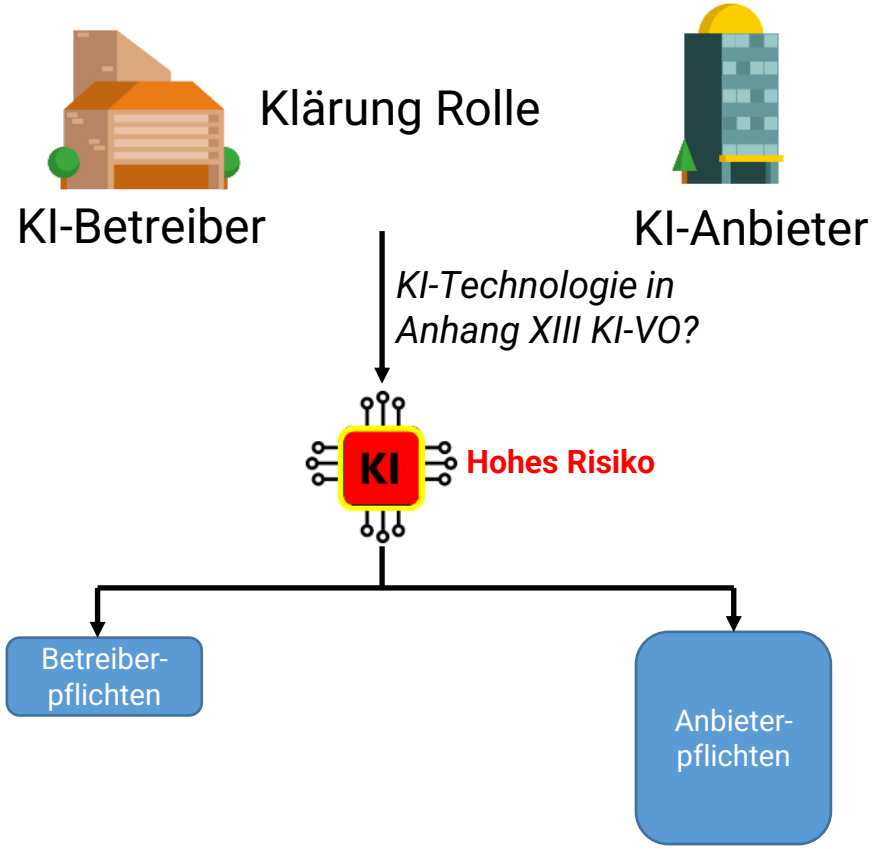
KI-VO



Wichtig: Nicht jede KI ist eine Hochrisiko-KI

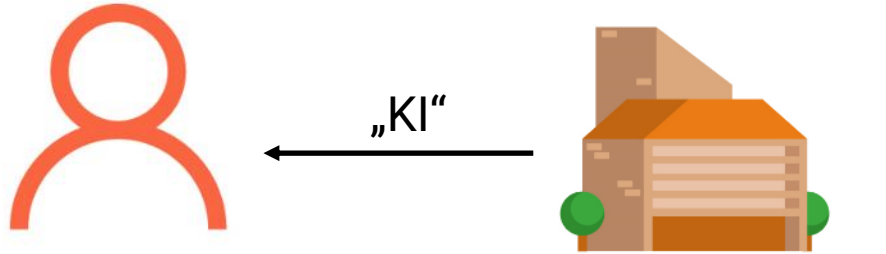
Umgang mit Hochrisiko-KI (nach DS-GVO und KI-VO)





Informationspflichten

Informationspflichten bei KI-Systemen



- Baustein des Rechts auf **informationelle Selbstbestimmung**
- Soll **weitere Betroffenenrechte** (z.B. Auskunft) ermöglichen

Rollen:

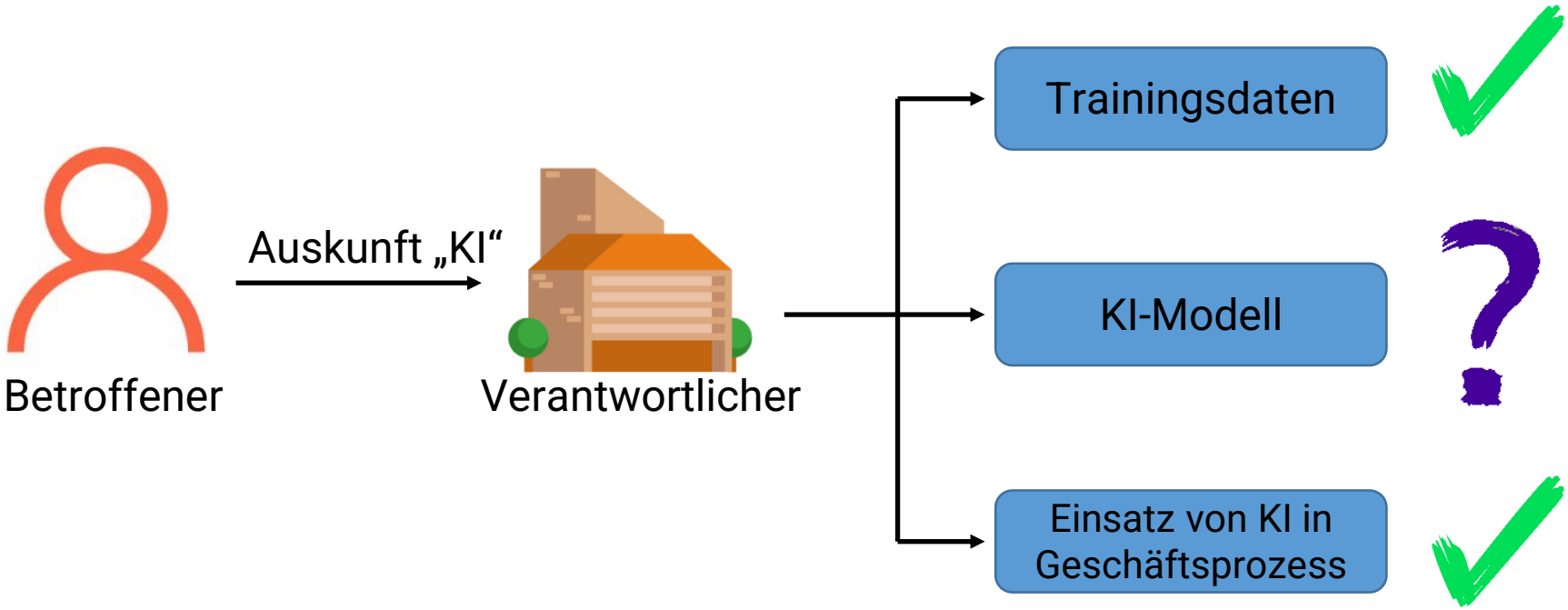
Betrieb einer KI-Anwendung → Im Prinzip **wie sonst** auch informieren (nur „mit KI“) ✓

Training eines KI-Modells → Je nach **Art der Datenquelle**:
- Direkterhebung
- Dritterhebung (Ausnahmeregelungen beachten)

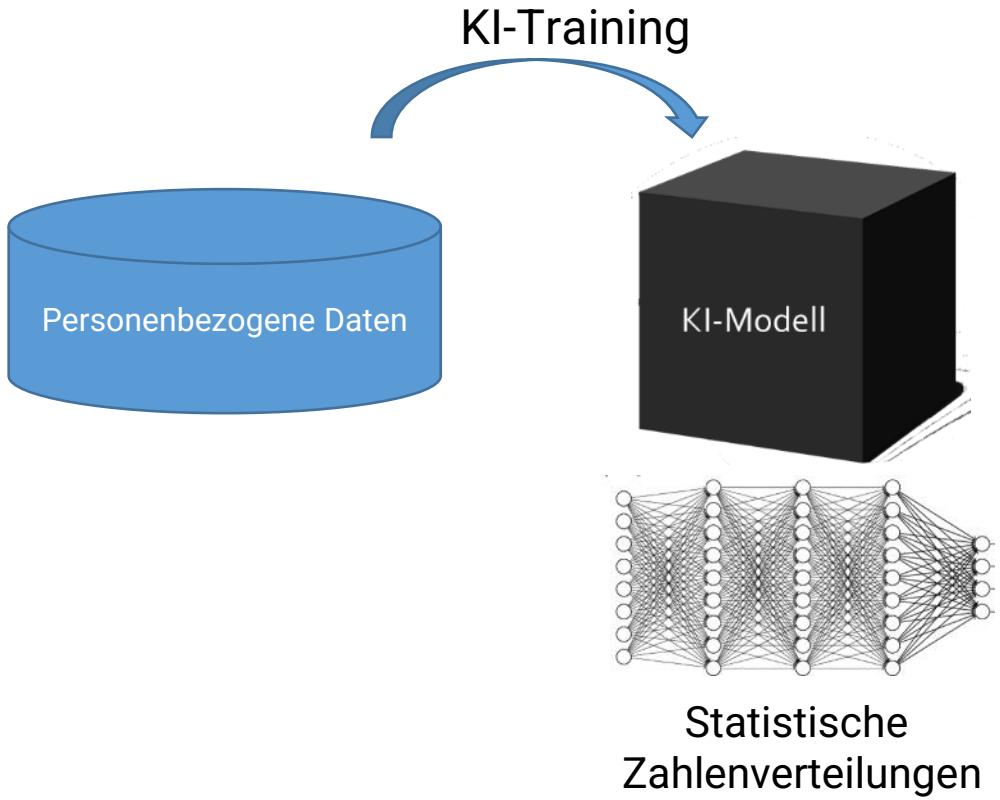
✓

Betroffenenrechte

Betroffenenrechte (Auskunft)



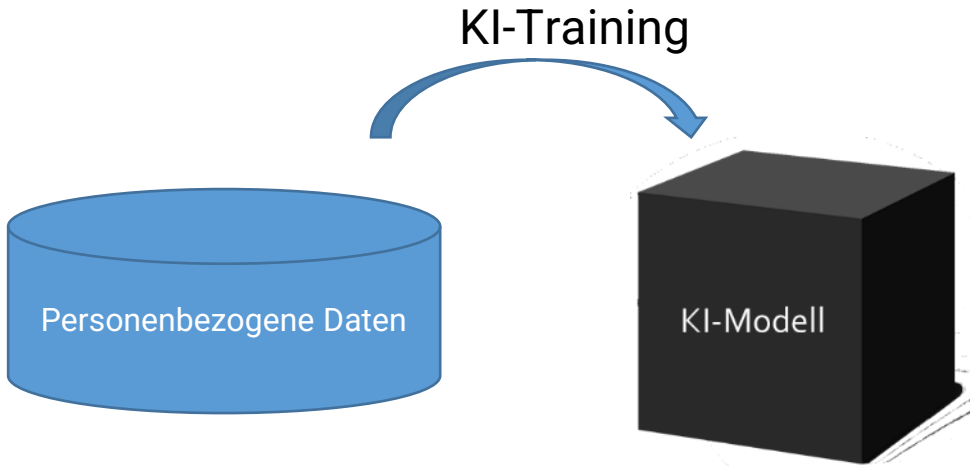
Betroffenenrechte (Auskunft KI-Modell)



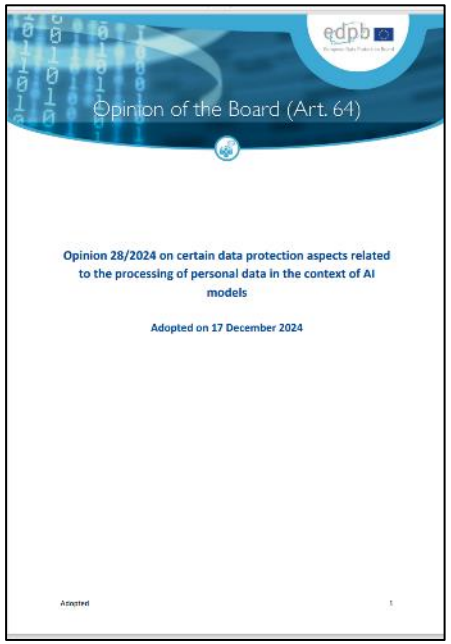
<u>Rahmenbedingungen:</u>

- Personenbezogene **Trainingsdaten**
- Nichtlineare maschinelle Lernverfahren (z.B. **Neuronale Netze**)
- Kodierung als **Zahlen(-vektoren)**
- Schrittweise **Lernverfahren**
- Es gibt durchaus **personenbezogen Ausgaben**
- Man kann aber meist **nicht** mal sagen, ob ein **konkretes** personenbezogenes Datum auch gelernt wurde

Betroffenenrechte (Auskunft KI-Modell)



„Kann sein", bewertet die zuständige Aufsichtsbehörde konkret im Einzelfall

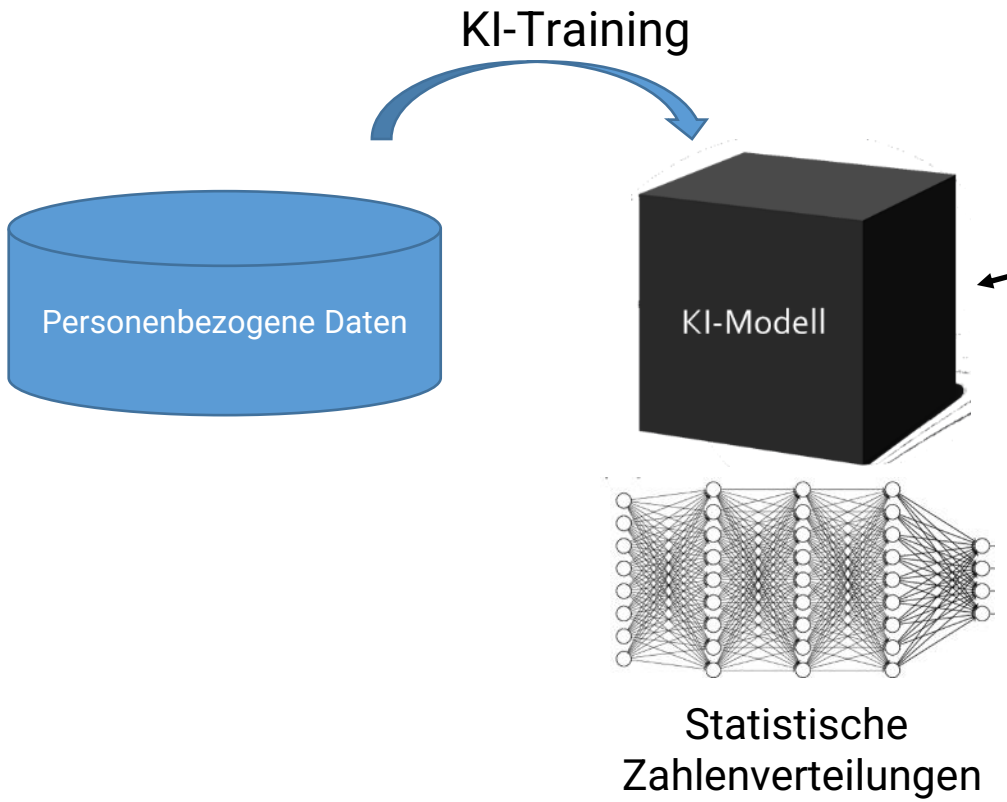


Gretchenfrage:

Ist ein KI-Modell als solches ein personenbezogenes Datum?

https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

Betroffenenrechte (Auskunft KI-Modell)



<u>Einordnung:</u>

- **Technisch** oder **praktisch** bei bestimmten KI-Modellen **nicht möglich**

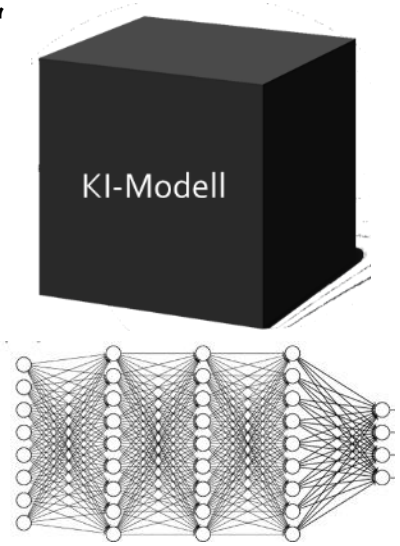
<u>Umgang in der Praxis:</u>

- Ggf. aus Trainingsdaten beauskunften (wenn KI-Anbieter)
- Ggf. auf KI-Anbieter verweisen (wenn KI-Betreiber)

Betroffenenrechte (Löschung KI-Modell)

Betroffener

„Bitte Löschen“ →



Statistische Zahlenverteilungen

Einordnung:

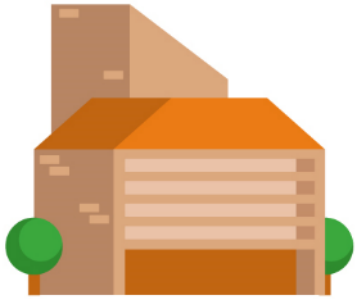
- **Technisch** oder **praktisch** bei bestimmten KI-Modellen **nicht möglich** (ohne das KI-Modell evtl. massiv zu schädigen)

Umgang in der Praxis:

- Löschdaten in Filter aufnehmen (wenn KI-Betreiber)
- Aus Trainingsdaten (nächste Produktversion) löschen (wenn KI-Anbieter)

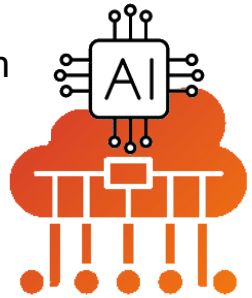
KI-as-a-Service

KI-as-a-Service



KI-Betreiber
(Verantwortlicher für den Einsatz von KI)

beauftragt



✓ Ist im Prinzip Datenschutz-"Standard":
- Auftragsverarbeitung (mit Vertrag)
- Bei sog. unsicherem Drittland: Geeignete Garantien
- Bsp: US-Dienstleister meist *EU-U.S. Data Privacy Framework*

! Bitte achtsam sein: **KI-Dienstleister** haben ggf. eigenes **Interesse** an **Nutzungsdaten** (für Produktverbesserung):
- *Zweckbindung sicherstellen (Vertrag)*
- *Zweckänderung rechtlich regeln (sofern gewollt) - schwierig*

Zusammenfassung

Zusammenfassung DS-GVO vs. KI-VO

- ☑ Datenschutz ist **Grundrechtsschutz** (auch bei KI) bei der Verarbeitung Ihrer Daten (DS-GVO)
- ☑ KI-Verordnung ist **KI-Produktregulierung** und Marktüberwachung
- ☑ Viele **Synergien** zwischen DS-GVO und KI-Betreiber (nach KI-VO)
- ☑ Bei KI-VO Voraussetzungen prüfen: **KI-System** nach KI-VO?
- ☑ Bei KI-VO Risikoklasse prüfen: Muss **überhaupt viel** nach KI-VO **gemacht werden?**
- ☑ **Rechtssicherheit** durch **Orientierungshilfen** der Datenschutzaufsichtsbehörden

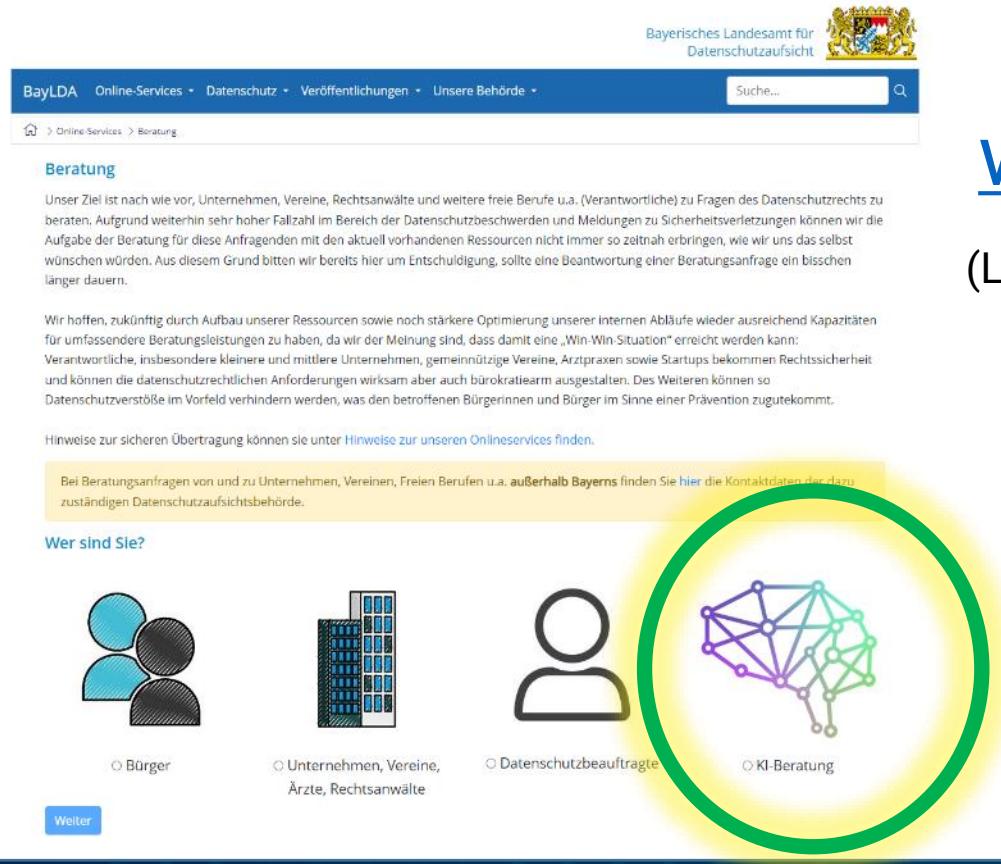
Checkliste *Künstliche Intelligenz und Datenschutz* (in 8 Schritten)

Checkliste Künstliche Intelligenz und Datenschutz (in 8 Schritten)

- ☑ **Anwendungsbereich** klären
- ☑ Rollen und **Verantwortlichkeiten** festlegen
- ☑ **Rechtsgrundlagen** finden
- ☑ **Privacy by Design** umsetzen
- ☑ **Hochrisiko-KI** in den Griff bekommen
- ☑ **Informationspflichten** erfüllen
- ☑ **Betroffenenrechte** (mit Blick auf KI) umsetzen
- ☑ **KI-as-a-Service** datenschutzkonform nutzen

Nebeneffekt von KI + Datenschutz:
Viele **Betreiberpflichten** nach KI-VO sind auch schon **umgesetzt**

Noch weitere Fragen?



www.lda.bayern.de/beratung

(Leider nur für Teilnehmerinnen und Teilnehmer aus Bayern)

Interesse an mehr Datenschutz?

- BIHK Webinarreihe *Datenschutz für Unternehmen*
- BIHK Ratgeber *Datenschutz und Künstliche Intelligenz - Darauf müssen Sie achten*
- BIHK/BayLDA Webinar *Künstliche Intelligenz und Datenschutz in der Praxis (Teil 2: Vertiefung) am 27. Februar 2024 - Anmeldung*

Vielen Dank für Ihre Aufmerksamkeit