KI und Datenschutz – Schnittstellen nutzen, Synergien erreichen

IHK-Veranstaltung „KI und Datenschutz in der Praxis – Best Practices für Unternehmen“ am 08.05.2025

Die DS-GVO bleibt unberührt – Art. 2 Abs. 7 KI-VO

KI-VO vs. DS-GVO

- Allerdings eine Vielzahl von Verweisen auf die DS-GVO
  - z.B. Definitionen „pbD“ „biometrische Daten“, „Profiling“
- Einhaltung der Datenschutzvorschriften ist Teil der KI-VO

Erw.Gr. 69:

„Das Recht auf Privatsphäre und den Schutz personenbezogener Daten

muss während des gesamten Lebenszyklus des KI-Systems sichergestellt sein“

Konformitätsbewertung:
„..wenn ein KI-System die Verarbeitung personenbezogener Daten erfordert, eine Erklärung darüber, dass das KI-System den Verordnungen (EU) 2016/679 und (EU) 2018/1725 sowie der Richtlinie (EU) 2016/680 entspricht“

- Art. 99 VII „Doppelbestrafung“

- **ABER:** DS-GVO gilt schon jetzt!!

KI-VO vs. DS-GVO

- **Die KI-VO gilt, jedoch nicht die DSGVO**
  (wenn keine personenbezogenen Daten verwendet werden, z. B. Schulungen zu anonymen Daten oder die Verwendung nicht personenbezogener Daten), in einigen Fällen in Verbindung mit dem einschlägigen sektoralen Recht, das für den Tätigkeitsbereich gilt, in dem das KI-System eingesetzt wird (z. B. Sicherheitsrecht und kritische Infrastruktur);

- **die DSGVO gilt, aber nicht die KI-VO**
  (z. B. wenn das KI-System speziell für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt oder in Betrieb genommen wird; bei quelloffenen Systemen, die unter freien und quelloffenen Lizenzen veröffentlicht werden;

- **sowohl die KI-VO, als auch die DS-GVO gelten**
  im Regelfall immer dann, wenn personenbezogene durch das KI- System oder Modell verarbeitet werden

Daten sind alles

KI und Datenschutz: Personenbezogene Daten

Personenbezug?

- Wurde mit pbD trainiert?
- Eingabe- und Ausgabewerte, Verknüpfung von Ausgabewerten mit pbD
- Ist ein KI- Modell personenbeziehbar? Personenbezug entfernt?(Anonymisierung durch Generalisierung?)
- EuGH- Rechtsprechung (Breyer, Deloitte)
  -> Besteht die Möglichkeit die pbD zu extrahieren?

Maßnahmen:

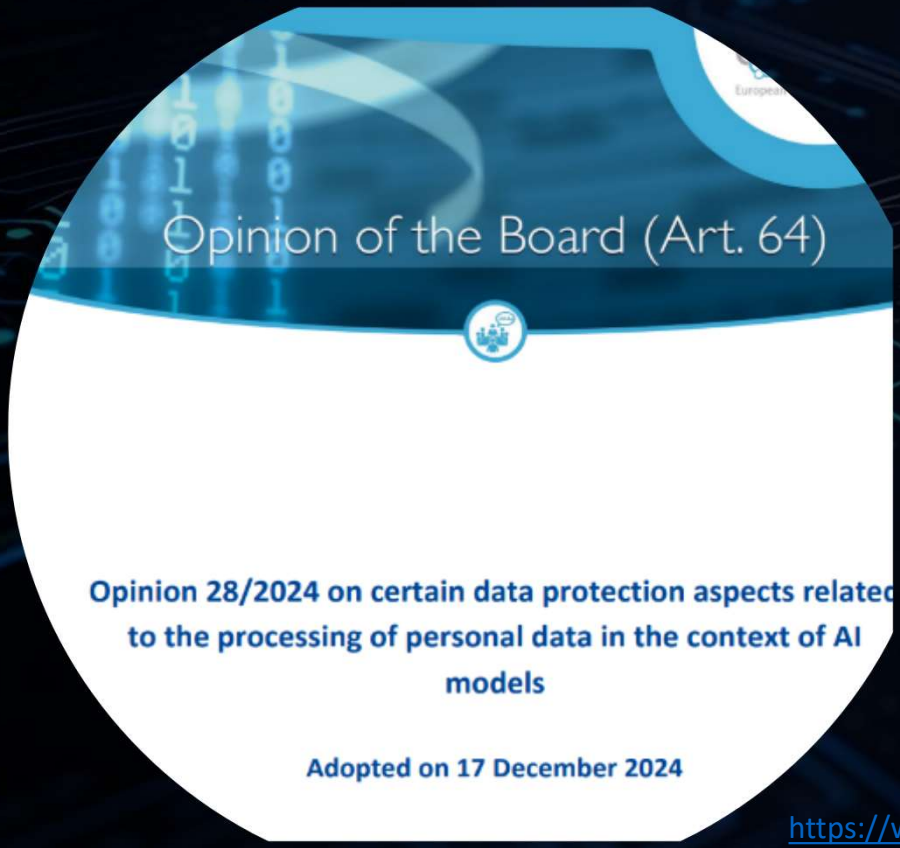
- Technik genau betrachten
- Anonymisierungsmöglichkeiten prüfen -> Wirklich anonym?
- Mitarbeiter schulen / KI- Richtlinie im Unternehmen
- Tools zur Erkennung von pbD (Namen, Orte, Mailadressen)

Bezug zur KI-VO:

- Art. 10 KI-VO Daten- Governance

KI und Datenschutz: Personenbezogene Daten

Opinion 28/2024 “on certain data protection aspects related to the processing of personal data in the context of AI models”



„Based on the above considerations, the EDPB considers that AI models trained on personal data ***cannot, in all cases, be considered anonymous****. Instead, the determination of whether an AI model* ***is anonymous should be assessed, based on specific criteria****, on a case-by-case basis.”*

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

KI und Datenschutz: Personenbezogene Daten

Personenbezug im KI- Modell?

- Trainingsdaten bleiben im Modell gespeichert -> mathematische Objekte
- Trainingsdatenpunkte können abweichen, aber ursprüngliche Informationen bleiben
- Direkte oder indirekte Extraktion bleibt möglich
- Rn. 31:

*„Whenever information relating to identified or identifiable individuals whose personal data was used to train the model may be obtained from an AI model with **means reasonably likely to be used**, it may be concluded that such a model is **not anonymous**."*

Wann kann von einer Anonymisierung ausgegangen werden?

- Personenbezug besteht auch bei Informationen die nur im maschinenlesenbaren- Format vorliegen
  -> keine automatische „Anonymisierung"
- Ausreichende Beweise ("sufficient evidence"), dass keine Extraktion pbD möglich

Der Zweck heiligt die Mittel?!

KI und Datenschutz: Zweckbestimmung

Besonderheiten beim Einsatz / Training von KI:

- Was passiert wann mit welchen Daten?
- Wo kommen die Daten her? (Internet, Unternehmen)
- Zu welchen Zweck/ in welchem Kontext wurden sie ursprünglich erhoben?
- Wofür möchte ich die KI verwenden ? („mal KI ausprobieren“ ist eher schwierig)
- Zweckänderung? (Art. 6 Abs. 4 DS-GVO Kompatibilitätsprüfung + Art. 6 Abs. 1 DS-GVO)

Maßnahmen:

- Einsatzfelder und Zwecke explizit VORHER festlegen

Bezug zur KI-VO:

- Wahl des Modells
- Auswahl der Trainingsdaten -> Art. 10 Abs. 2 KI-VO *„…für die Zweckbestimmung…geeignet…“*
- Zweckbestimmung zur Klassifizierung erforderlich -> Art. 6 Abs.2 KI-VO
- Zwecke nach der KI-VO zulässig? -> Art. 5 KI-VO
- Risikomanagement -> Mögliche Fehlanwendungen -> Art. 9 KI-VO

Das (rechtliche) Fundament

KI und Datenschutz: Rechtsgrundlagen – Einwilligung

Training/ Einsatz von KI:

- Auch KI-Verarbeitungen brauchen eine Rechtsgrundlage
- Trennung der einzelnen Verarbeitungsphasen
- Art. 6 Abs. 1 lit. a DS-GVO Einwilligung
  - Automatisierte Sammlung -> Betroffene oftmals nicht bekannt
  - Widerruflichkeit der Einwilligung
  - „informierte“ Einwilligung
  - Einsatz: denkbar -> Aber: Verwendung zur Weiterentwicklung?

- Bei Art. 9- Daten: Sonderregelungen oder Einwilligung

Maßnahmen:

Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz – LfD Baden- Württemberg
https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/

Bezug zur KI-VO:

- Art. 10 Abs. 5 KI-VO: Verarbeitung besonderen Daten für Korrektur von Verzerrungen, Art. 59 KI-VO

KI und Datenschutz: Rechtsgrundlagen

Art. 6 Abs. 1 lit. b DS-GVO - Vertragserfüllung:

- Zur Erfüllung des Vertrags „erforderlich“ -> reine Nützlichkeit reicht nicht aus
- Klar erkennbar
- Zweckbindung -> keine Weiterentwicklung
- Beispiele: Behandlungsvertrag, KI- Sprachgenerator

Art. 6 Abs. 1 lit. c DS-GVO – Gesetzliche Verpflichtung:

- Beschränkt auf das absolut Notwendige
- Rechtlich angeordnete Pflicht / Rechtsprechung -> kein Entscheidungsspielraum

Art. 6 Abs.1 lit. d DS-GVO – lebenswichtige Interessen:

- Kein milderes Mittel
- Kurzfristige Maßnahmen in Notsituationen

KI und Datenschutz: Rechtsgrundlagen – Berechtigtes Interesse

Training / Einsatz von KI:

- Opinion 28/2024
- Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Drei- Stufen- Test:

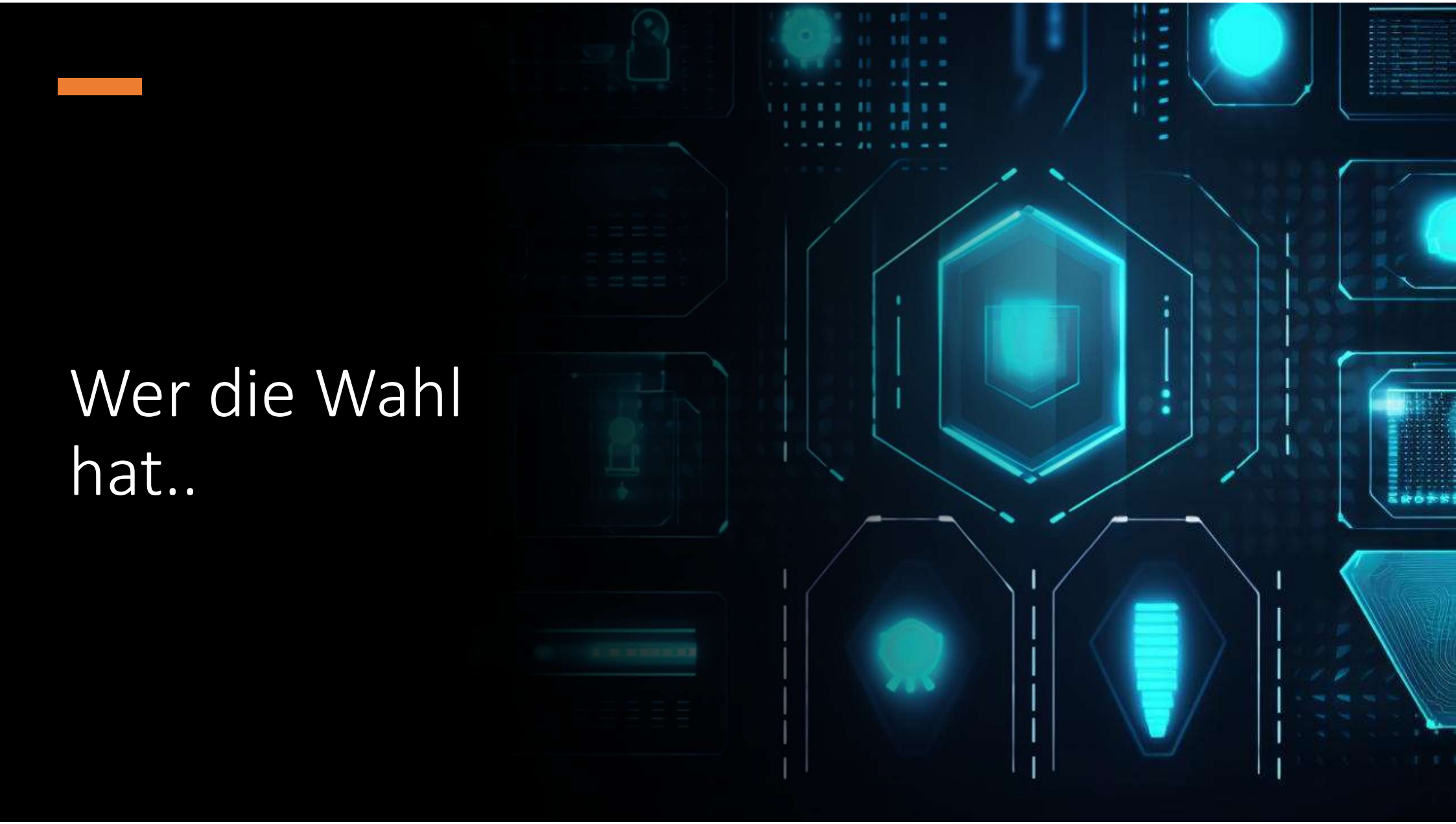
- Berechtigtes Interesse des Verantwortlichen / eines Dritten
- Notwendigkeit der Verarbeitung (“necessary”)
- Interessensabwägung

- Widerspruchsrecht
- „Kein milderes Mittel“
- Erwartbarkeit für Betroffene?

Riskominimierende Maßnahmen:

- Guidelines Pseudonymisation 01/2025 https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf
- Technische und organisatorische Maßnahmen

Wer die Wahl hat..



KI und Datenschutz: Rechtsgrundlagen – The fruit of the poisonous tree?

Nutzung eines rechtswidrig trainierten Modells – Datenschutzkonform möglich?

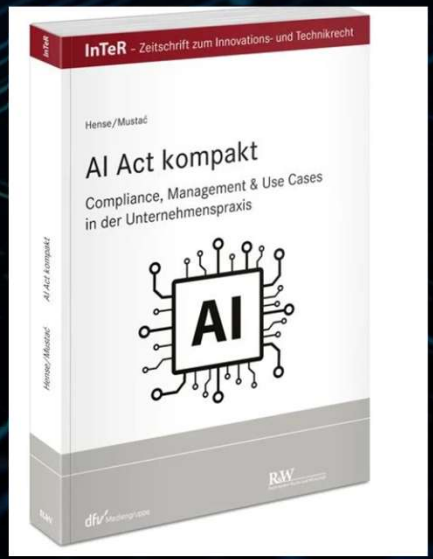
- Opinion 28/ 2024
- Feststellung der datenschutzrechtlichen Rollen
- Jeder Verantwortliche muss die Rechtmäßigkeit der von ihm zu verantwortenden Datenverarbeitung sicherstellen und nachweisen können
- Hat der Verantwortliche geprüft, ob das Modell rechtswidrig trainiert wurde?
- Offensichtlich rechtswidrig?
  ->Von einem Gericht oder einer Behörde festgestellt
- Einbeziehung des Trainings in die Interessensabwägung

- Bußgeld der italienischen Aufsichtsbehörde gegen OpenAI?

KI und Datenschutz: Auswahl eines KI - Systems

Due Dilligence des Betreibers eines Hochrisiko- KI- Systems:

- Ist das KI- System in der EU- Datenbank für Hoch-Risiko- KI- Systeme registriert?
- Liegen Zertifizierungen von nationalen oder internationalen Normungsorganisationen vor?
- Wurde das KI- System einer Konformitätsbewertung unterzogen?
- Hat das KI- System eine CE- Konformitätskennzeichnung?
- Liegt eine geeignete Betriebsanleitung vor?



AI Act kompakt - Compliance, Management & Use Cases in der Unternehmenspraxis
Von: Peter Hense & Tea Mustac

No risk, no fun?

KI und Datenschutz: Datenschutzfolgenabschätzung

Besonderheiten beim Einsatz / Training von KI:

In den meisten Fällen erforderlich

- Z.B.„Muss“: Steuerung Interaktion mit Betroffenen -> Chatbot
- Hilfestellung: „Ethik-Leitlinien für eine vertrauenswürdige KI“ https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
- Modellrisiken: Mangelhafte Anonymisierung, Diskriminierung, Memorization…
- Einsatzrisiken: Unrichtige Ausgaben, Betroffenenrechte, Fehlende Eingriffsmöglichkeit

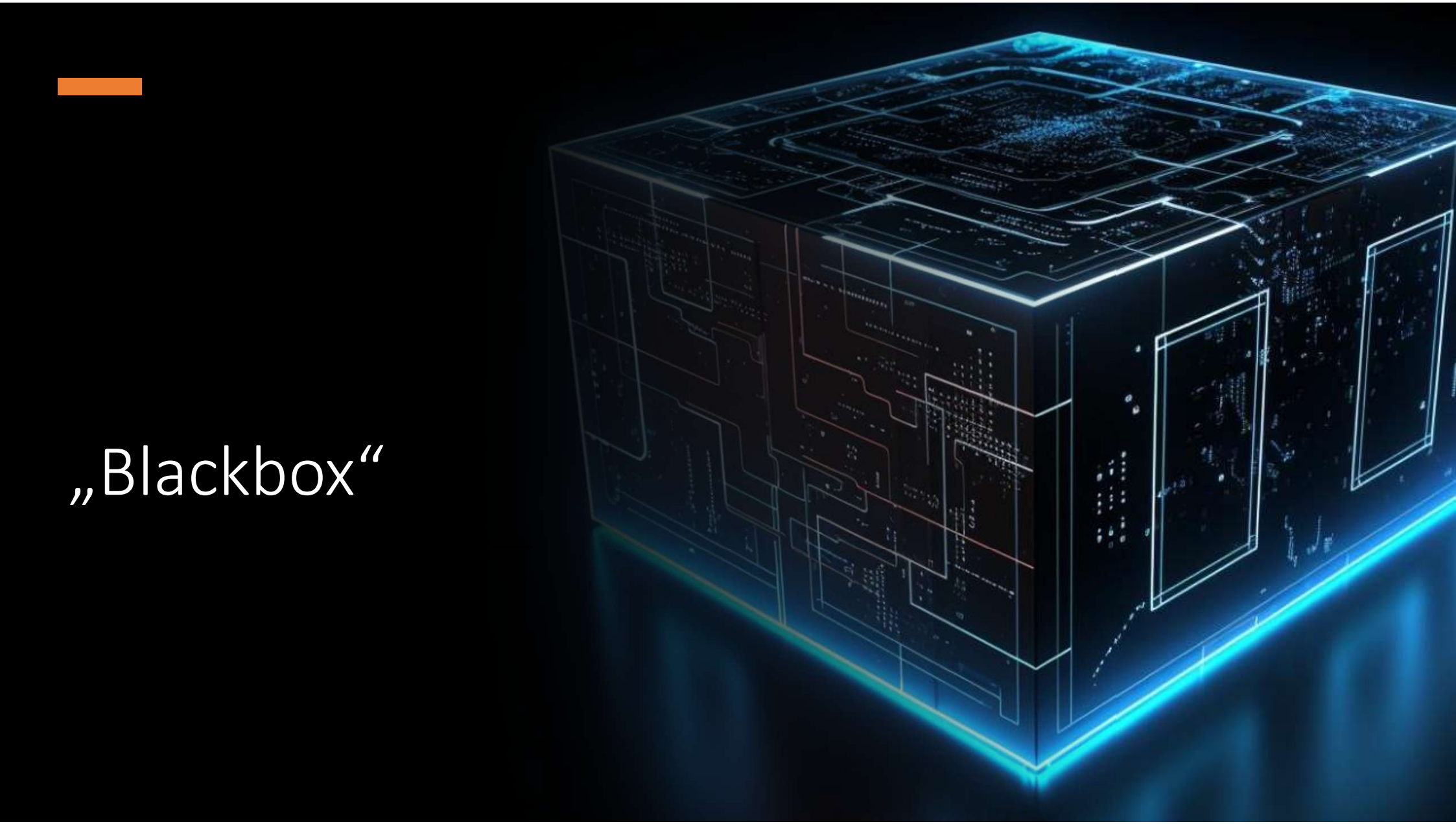
Maßnahmen:

- „Schwellwertprüfung“ / Prüfen, ob eine DSFA durchgeführt wurde
- technische Maßnahmen: https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

Bezug zur KI-VO:

- Risikomanagementsystem (Art. 9 KI-VO) , Art. 26 Abs. 9 KI-VO Weiterverwendung Art. 13 KI-VO-Informationen

„Blackbox“



KI und Datenschutz: Informationspflichten / Transparenz

Besonderheiten beim Einsatz / Training von KI:

- Art. 13 Abs. 2 lit. f) DS-GVO in Bezug auf Art. 22 DS-GVO
  „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“
- Generierung von Informationen über Dritte / Abruf von Daten Dritter
- KI-as-a-Service (Abhängigkeit von Dritten)

Maßnahmen:

- Ausnahmen von der Informationspflicht sorgfältig prüfen
- Zumindest so verständlich wie möglich darstellen

Bezug zur KI-VO:

- Art. 13 Abs. 1, 2 KI-VO Bereitstellung einer Gebrauchsanweisung
- Art. 50 KI-VO (für alle), Art. 26 VII und IX, Art. 86 KI-VO
- Transparenz im Sinne der KI-VO (Erw.Gr. 27, 72)

KI und Datenschutz: Die Betriebsanleitung Art. 13 KI- VO

Mindestinhalte:

- Identität und Kontaktdaten des Anbieters (und seines bevollmächtigten Vertreters)
- Merkmale, Fähigkeiten, Grenzen und Verwendungszweck des KI- Systems
  - Grad der Genauigkeit, Robustheit und Cybersicherheit mit dem getestet und validiert wurde
  - Alle bekannten und vorhersehbaren Umstände die zu Risiken führen können
  - Technische Fähigkeiten und Merkmale
  - Leistung des KI- Systems
  - Informationen zu Trainings- Validierungs- und Testdatensätzen

- Vorgesehene Menschliche Überwachungsmaßnahmen
- Erforderliche Rechen- und Hardwareressourcen
- Voraussichtliche Lebensdauer
- Beschreibung der Protokollierungsmechanismen

KI und Datenschutz: Art. 53 KI-VO i. V. m. Anhang XI

Technische Dokumentation GPAI:

- Allgemeine Beschreibung
  - Aufgaben die das Modell erfüllen soll
  - Architektur und Anzahl der Parameter
  - Modalität und das Format der Ein- und Ausgaben
- Ausführliche Beschreibung der Elemente des Modells
  - Technische Mittel (Betriebsanleitungen)
  - Entwurfsspezifikationen / Trainingsmethoden
  - Informationen über Trainingsdaten (Art, Herkunft und Aufbereitungsmethode)
  - Rechnerressourcen
- Transparenzinformationen Anhang XII

Zeit für Ihre Fragen!

Carolin Loy
Bereichsleitung Digitalwirtschaft und Rechtsfragen Künstlicher Intelligenz
Pressesprecherin / Beauftragte für Öffentlichkeitsarbeit
Bayerisches Landesamt für Datenschutzaufsicht

E-Mail: carolin.loy@lda.bayern.de
https://www.lda.bayern.de/ki