

Abschlussreview zum Projekt TAHAI

Rechtliche und ethische Fragen des KI-Einsatzes

Prof. Dr. Ralf Schnieders
20. Mai 2025
in Berlin



**Hochschule für Technik
und Wirtschaft Berlin**

University of Applied Sciences

Agenda

- 1 Anwendungsszenario 1: Mediationsprotokolle
- 2 Anwendungsszenario 2: Graffiti-Videoerkennung
- 3 Erkenntnisse

Agenda

- 1 **Anwendungsszenario 1: Mediationsprotokolle**
- 2 Anwendungsszenario 2: Graffiti-Videoerkennung
- 3 Erkenntnisse

Problembereich Datenüberlassungsvertrag

- Regelungen
 - zur Inhaberschaft/Lizenzierung,
 - zur Qualität/Haftung,
 - zu datenschutzrechtlichen Anforderungen
- Bei personenbezogenen Daten: Anforderungen der DSGVO
- Regeln der DSGVO über gemeinsame Verantwortung (Art. 26)
- Musterverträge zu Datenüberlassungsverträgen
- Eigenes Projekt der Fraunhofer IOSB / FH Bielefeld zu dem Thema
- Urheberrechtlicher Inhalt: Regelungsbedarf hinsichtlich:
Inhaberschaft / Lizenzierung für: überlassene Daten, Ergebnisse der Datenverarbeitung, geschulte KI.

Art. 26 DSGVO

Gemeinsam Verantwortliche

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Datenschutzrechtliche Vertragsinhalte

- Was kraft Gesetzes insb. zu regeln ist:
 - Betroffene Person muss ihre Rechte bei jedem Verantwortlichen geltend machen können.
 - „Transparenz“: Genaue Definition der behandelten Daten: Welche personenbezogenen Daten, in welchem Prozessabschnitt, wie genau behandelt?
 - Namentlich benannte Ansprechpartner eines datenschutzrechtlichen Verantwortlichen mit Kontaktdaten
 - Vorsehen eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO
 - Grundsatz der Datenminimierung: Nur zwingend erforderliche Daten dürfen verarbeitet werden bzw. müssen ansonsten gelöscht werden
- Grunddilemma: Wie Anforderungen realitätsnah erfüllen?
- Vertragspartner/Verantwortlich ist die Hochschule!

Problembereich Datennutzung

- Bei personenbezogenen Daten: Anforderungen der DSGVO
- Erlaubnis für die Verarbeitung personenbezogener Daten muss vorliegen: Einwilligung der betroffenen Person? Auch in die Verarbeitung mittels API-KI? Problematik der Einwilligung
- Rechte der betroffenen Person, insb.:
 - Recht auf Auskunft
 - Recht auf Berichtigung
 - Recht auf Löschung
- Wie sicherstellen gegenüber API-KI-Anwendungen (AGB)?
- Begrenzte Bedeutung von Privilegierungen wiss. Verarbeitung, Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 4 Abs. 1, § 6, § 37 Berliner Hochschulgesetz sowie § 17 Berliner Datenschutzgesetz: Interessenabwägung!

Anonymisierung

- Die Lösung für die datenschutzrechtlichen Anforderungen: Anonymisierung?
- Hohe Anforderungen: Ausschluss der Identifizierbarkeit mit zumutbarem Aufwand
- Gruppenzugehörigkeiten
- Problem: Bleiben (mittels Generalisierung etc.) anonymisierte Daten weiter ausreichend aussagekräftig?
- Reicht eine Wahrscheinlichkeit von 95%, dass aller Personenbezug entfernt wurde (nach Behandlung mit Anonymisierungs-Tool)?
- Bei einer Behandlung mittels KI? Bei ständig steigender Leistung der KI?

Agenda

- 1 Anwendungsszenario 1: Mediationsprotokolle
- 2 Anwendungsszenario 2: Graffiti-Videoerkennung**
- 3 Erkenntnisse

Problembereich Datenschutz?

- Spezialgesetzliche Anforderungen an die Videoüberwachung: §§ 27, 29 Bundespolizeigesetz, § 4 Bundesdatenschutzgesetz
- Spezielle gesetzliche Grundlage für die KI-gestützte Videoauswertung erforderlich?
- In unserem speziellen Anwendungsfall wohl keine personenbezogenen Daten → keine datenschutzrechtlichen Anforderungen

§ 27 Bundespolizeigesetz

Selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte

Die Bundespolizei kann selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte einsetzen, um

1. unerlaubte Grenzübertritte oder Gefahren für die Sicherheit an der Grenze oder
2. Gefahren für die in § 23 Abs. 1 Nr. 4 bezeichneten Objekte oder für dort befindliche Personen oder Sachen

zu erkennen. In den Fällen des Satzes 1 Nr. 2 muß der Einsatz derartiger Geräte erkennbar sein. Werden auf diese Weise personenbezogene Daten aufgezeichnet, sind diese Aufzeichnungen in den Fällen des Satzes 1 Nr. 1 spätestens nach zwei Tagen und in den Fällen des Satzes 1 Nr. 2 spätestens nach 30 Tagen zu vernichten, soweit sie nicht zur Abwehr einer gegenwärtigen Gefahr oder zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt werden.

Problembereich EU AI Act (KI-VO)

- Für die KI-gestützte Videoauswertung
- Risikobasierter Ansatz der KI-VO:
 - Verbot von KI mit unannehmbarem Risiko (Z.B. biometrische Echtzeit-Fernidentifikation zu Strafverfolgungszwecken),
 - Hochrisiko-KI-System → Spezielle Anforderungen und Bewertung (als spezielles Produktsicherheitsrecht),
 - Bloße Transparenzanforderungen für sonstige KI-Anwendungen
- Hier insbes. wohl keine Einordnung als Emotionserkennungssystem (Art. 6 Abs. 2 in Verbindung mit Anhang III Nr. 1 lit. c)
- Daher nur allgemeine Informationspflicht nach Art. 50 Abs. 1, dass der Nutzer mit einer KI interagiert.

Anhang III KI-VO

Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2

Als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 gelten die in folgenden Bereichen aufgeführten KI-Systeme:

1. Biometrie, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

a) biometrische Fernidentifizierungssysteme.

Dazu gehören nicht KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, verwendet werden sollen;

b) KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen;

c) KI-Systeme, die bestimmungsgemäß zur Emotionserkennung verwendet werden sollen.

Art. 50 KI-VO

Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme

(1) Die Anbieter stellen sicher, dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Diese Pflicht gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme, wenn geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen, es sei denn, diese Systeme stehen der Öffentlichkeit zur Anzeige einer Straftat zur Verfügung.

Agenda

- 1 Anwendungsszenario 1: Mediationsprotokolle
- 2 Anwendungsszenario 2: Graffiti-Videoerkennung
- 3 **Erkenntnisse**

Erkenntnisse

- Im Projekt schwerpunktmäßige Relevanz des Aspektes Datenschutz
- Erfüllung der datenschutzrechtlichen Anforderungen als praktische Herausforderung
- Insbesondere sind die beteiligten Universitäten nur bedingt in der Lage, mit den heutigen datenschutzrechtlichen Anforderungen an das Forschungsmanagement umzugehen
- Anonymisierung als Lösung?
- Unterschiedliches Verständnis bei Juristen und Ingenieuren
- Umgang mit rechtlicher Unsicherheit

Erkenntnisse (2)

- EU AI Act (KI-VO) nur in speziellen Anwendungsfällen relevant
- Gerade für API-KI-Anwendungen kann KI-VO besondere (nicht im Rahmen von TAHA I sich stellende) Fragestellungen aufwerfen, weil KI-Anwendung erst durch Verwendung zu einem bestimmten Zweck zu einem KI-Hochrisiko-System werden kann
- Ethische Fragestellungen im Projekt nicht im Vordergrund.
Fragestellung: Ist die KI-Verarbeitung der hochsensiblen Mediationsdaten auch im Hinblick auf den weiteren Fortschritt vertretbar? Lösung über abgeschlossenes System und nur häppchenweise Eingabe.



Vielen Dank für die Zusammenarbeit!

www.htw-berlin.de

htw

**Hochschule für Technik
und Wirtschaft Berlin**

University of Applied Sciences