Einsatz von KI in der Verwaltung – unter Berücksichtigung datenschutz- und verkehrsrechtlicher Aspekte

3. Oktober 2024

Dr. Heidi Scheichenbauer

Research Institute AG & Co KG
Digital Human Rights Center
Florianigasse 55/10, 1080 Wien
www.researchinstitute.at

Research Institute

Digital Human Rights Center

FORSCHUNG

Interdisziplinäre Forschung zu Datenschutz, Datensicherheit und technischer Innovation

Technikfolgen-Abschätzung und Evaluationen

Bedarfs- und Akzeptanzanalysen

CONSULTING

Beratung zu rechtlichen, technischen und organisatorischen Fragen im Bereich Datenschutz sowie Netz- und Informationssicherheit

Datenschutz-Governance, Rechts- und Netzpolitik

Maßgeschneiderte Gutachten, Projekte & Lösungen

LEHRE

Seminare, Tagungen & Konferenzen

Vorträge & In-house-Schulungen

Akademische Lehre & wissenschaftliche Publikationstätigkeit

DR. IUR. HEIDI SCHEICHENBAUER

- Juristin
- **Senior Researcher** und **Senior Consultant**, Research Institute
- Autorin von Fachbeiträgen in datenschutzrechtlichen Fachzeitschriften (Jus-IT, Datenschutz-konkret)
- Mitautorin mehrerer aktueller Bücher zur Datenschutz-Grundverordnung (jusIT Spezial: DS-GVO, Handbuch Datenschutz Verlag WEKA) Vortragstätigkeiten
- Datenschutz für Vereine (Verlag Linde)
- Der Datenschutzbeauftragte (Verlag Linde)
- **Erfahrungen** in:
  - Wissenschaft und Consulting (RI, KMU Forschung Austria)
  - Interessenvertretung und Rechtsberatung (Fundraising Verband Austria)
- **Forschungsschwerpunkte**:
  - Datenschutzrecht für gem. Organisationen
  - Geodaten

KI IST IN DER VERWALTUNG ANGEKOMMEN

KI zur **Effizienzsteigerung**, **ressourcenschonender Bewältigung wiederkehrender Aufgaben** und **Lösung komplexer Probleme**

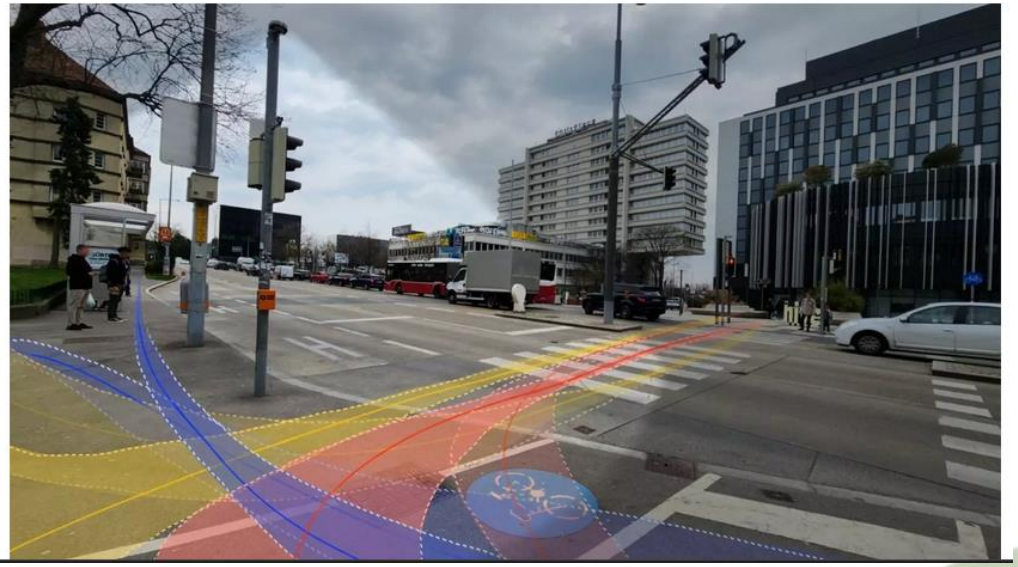
- **Chatbots** (*natural language processing*)
  - Stärkung der Behördenkommunikation
- **Intelligente Suchmaschinen**
  - Unterstützung von Benutzer:innen bei Auswertung sowie Strukturierung von Daten für Entscheidungen und Handlungsweisen
- **Prognosemodelle**
  - Vorhersagen von Hochwasserereignissen oder Krankheitsausbreitungen
- **Betrugsbekämpfungs-KI (PACC)**
  - KI als Technologie für Risikomanagement
- **Content-Erstellung**
  - Broschüren etc
- **Verkehrswesen**
  - Autonomes Fahren, Verkehrsmanagement

KI IST IN DER VERWALTUNG ANGEKOMMEN

KI an der Kreuzung

Wie KI hilft Wartezeiten, riskante Überquerungen bei Rot und unnötige Autostopps signifikant zu reduzieren: Die smarte Wiener Ampel erkennt von Weitem, ob Fußgänger über die Straße möchten und gibt ihnen grünes Licht.

Matilda Jordanova-Duda / 26.03.2024 / 10 Minute(n) /



https://www.relevant.news/ki-an-der-kreuzung/

STATUS QUO

- Einsatz von KI durch Verwaltungsbehörden selten explizit in nationalen Rechtsordnungen abgebildet
- prominentes europäisches Beispiel einer KI-Regelung betreffend den Einsatz von KI im öffentlichen Bereich "SyRI“ zur Aufdeckung von Betrug mit Sozialhilfeleistungen
- Einsatz beruhte auf einer speziellen Ermächtigungsgesetzgebung (Syri-Gesetz)
- Regelung wurde aufgehoben
  - Verstoß gegen Art 8 Abs 2 EMRK,
  - unverhältnismäßiger Eingriff,
  - zudem fehlende Transparenz über Funktionsweise

PRAXISBEISPIEL DEFALSIF-AI

- **Geplante Einsatzzwecke:**
  - Defalsif-AI adressiert im Kontext medienforensischer Werkzeuge (Hybrid-Threats – Fake-News) insbesondere politisch motivierte „**Desinformation“ bzw. „Fake News“**, welche politische sowie staatliche Institutionen unserer Demokratie – z.B. Wahlbeeinflussung – und somit letztlich das öffentliche Vertrauen in politische und staatliche Institutionen schwächt bzw. bedroht. Die inhaltlichen Forschungsschwerpunkte lagen auf audiovisueller Medienforensik, Textanalyse und deren multimodaler Fusion unter Zuhilfenahme von Methoden der Künstlichen Intelligenz (KI).

PRAXISBEISPIEL DEFALSIF-AI

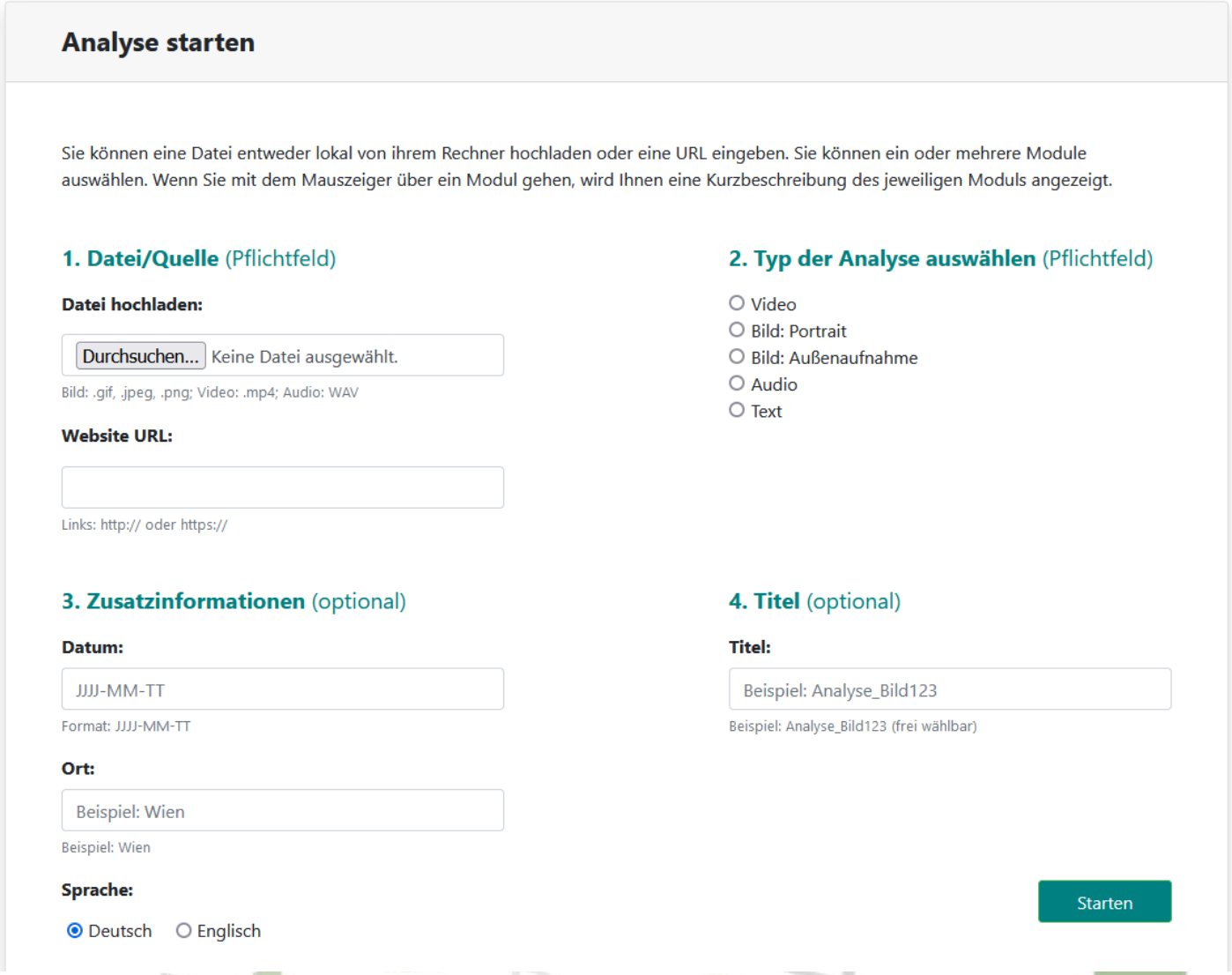
https://science.apa.at/project/defalsifai/

Praxisbeispiel DEFALSIF-AI

Wünsche der ministeriellen Bedarfsträger

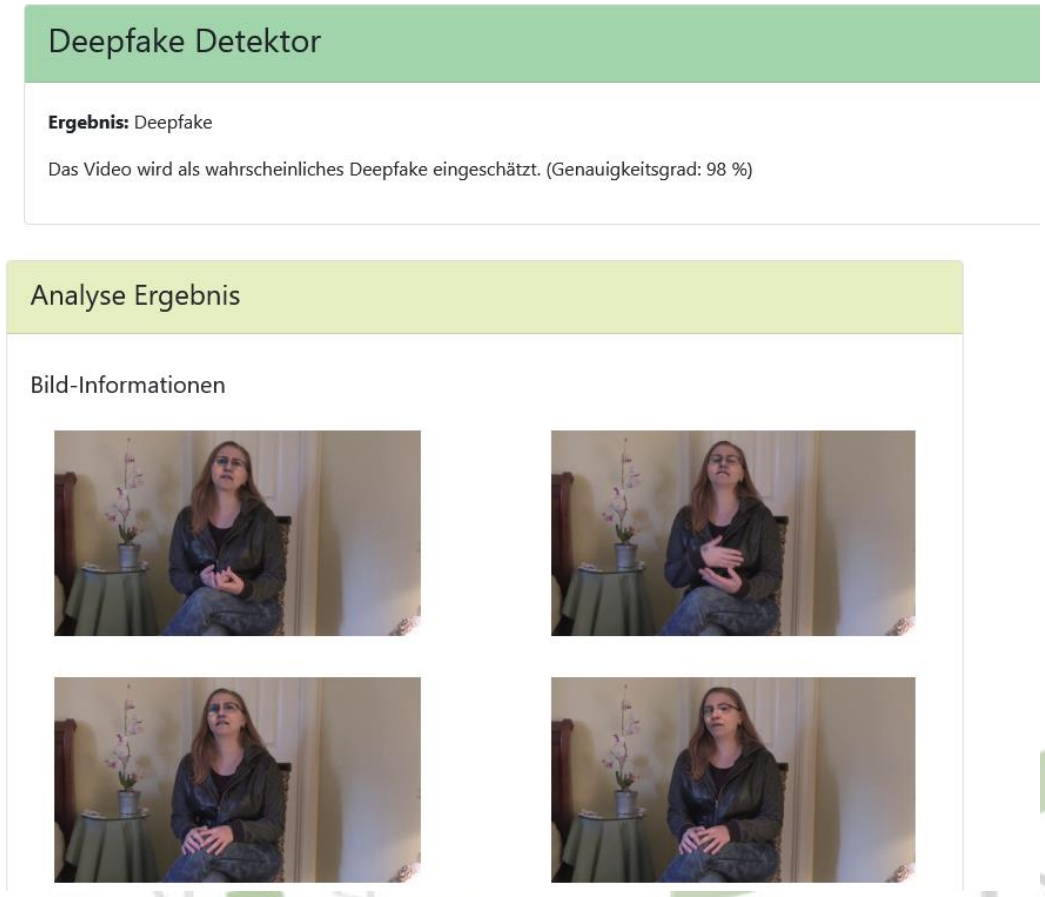
- **Identifikation von Narrativen in Nachrichten von Social Media,** um die Möglichkeit zu haben, **auffällige Widersprüche zu bekannten Positionen** (z.B. EU-Statements) zu erkennen.
- **regelmäßiger Report über Desinformation** im Kontext der österreichischen Außenpolitik um einen Überblick zu bekommen und gegebenenfalls gegensteuern zu können.
- **Auch sollen Informationen aus dem Internet ad hoc auf Desinformation überprüft werden können.**
- **Erkennung von Trending Topics aus anderen Ländern** (z.B. Brasilien: zuerst Covid-Schwerpunkt, daraus wurde Schwerpunkt zu Impfung) zu analysieren, um so einen Eindruck über für Österreich aufkommende Topics zu erhalten und sich für zukünftige Topics frühzeitig vorbereiten zu können
- **Wunsch eingehende Meldungen (Berichte, Nachrichten) die potentiell Falschnachrichten darstellen, in einem automatischen Pre-Processing gekennzeichnet (ge-flagged) haben, um bei der manuellen Verarbeitung Ressourcen zu sparen.**

DEFALSIF-AI: VERWIRKLICHTE MODULE

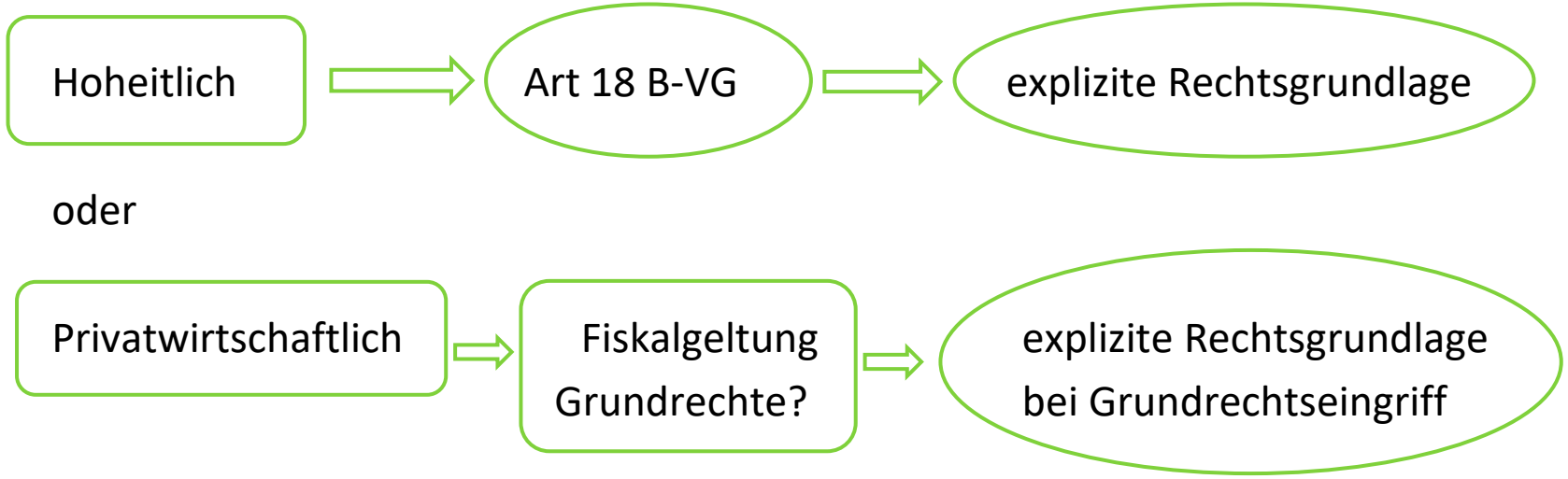


DEFALSIF-AI: VERWIRKLICHTE MODULE

- Video Module:
  - Deepfake-Worker: Das Deepfake-Modul dient der Erkennung von durch Deep-Fake-Verfahren erzeugten Manipulationen in Videos.



DEFALSIF-AI: EINORDNUNG VERWALTUNGSHANDELN



DEFALSIF-AI: EINORDNUNG VERWALTUNGSHANDELN

- Wie ist der Einsatz der KI-Anwendung verwaltungsrechtlich einzuordnen?
- Schlicht-hoheitliche Verwaltungsakte sind jene Verwaltungsorganhandlungen, die kein Hoheitsakt ieS (Verordnung, Bescheid, Befehl- oder Zwangsgewalt) sind, aber funktionelle Verbindung zur staatlichen Hoheitsverwaltung: „informelles Verwaltungshandeln“

ODER

- Privatwirtschaftsverwaltung: keine gesetzliche Ermächtigung, oft Vertrag, oft Abgrenzung nach Rechtsschutz

EINORDNUNG VERWALTUNGSHANDELN

Welche Bedingungen sind an das Verwaltungshandeln geknüpft?

- **Art 18 Abs 1 B-VG Legalitätsprinzip**: *„Die gesamte staatliche Verwaltung darf nur auf Grund der Gesetze ausgeübt werden*. […]“ (formeller Gesetzesvorbehalt)

- Grundrechtseingriffe: zB **§ 1 Abs 2 DSG, Art 8 Abs 2 EMRK**:

„(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, ***insoweit dieser Eingriff gesetzlich vorgesehen ist*** *und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist*.“ (formeller und materieller Gesetzesvorbehalt)

EINORDNUNG VERWALTUNGSHANDELN

- Aus dem Legalitätsprinzip ergibt sich, dass das Verwaltungshandeln sowohl inhaltlich als auch formell durch den Gesetzgeber determiniert sein muss
- Jeder Vollzugsakt muss formell und materiell auf das Gesetz zurückführbar sein
- Gleichzeitig wird ein großer Teil des Verwaltungshandelns nicht unmittelbar in Gesetzen beschrieben
- auch hier wird dennoch nicht im gesetzesfreien Raum agiert
- Tätigkeit erfolgt häufig auf Grund allgemeiner Aufgabenbestimmungen
- Verwaltung wird auch in diesen Fällen „auf Grund der Gesetze“ ausgeübt
- Judikatur hinsichtlich der erforderlichen Ausgestaltung dieser Rechtsgrundlagen ist schwankend und schwer in generelle Formeln zu fassen
- strenge Anforderungen an den Determinierungsgrad der Eingriffsnormen jedenfalls bei Grundrechtseingriffen
- „spezifische Determinierungspflicht“ und „Regelungsdichte“ geht über die allgemeinen Anforderungen des Art 18 Abs 1 B-VG hinaus

K600.053-023/0002-DVR/2008 Salzburger Fußgängerzone

- An sechs Einfahrtspunkten zur Salzburger Altstadt sollten Kennzeichen aller in die Fußgängerzone einfahrenden Kraftfahrzeuge (Kfz) elektronisch aufgezeichnet werden.
- Mittels spezieller Software sollte jedes aufgenommene Kennzeichen mit den in der „White list“ gespeicherten Datensätzen abgeglichen:
  - 1. „Erkennt“ das EDV-System das Kennzeichen als ein in der „White list“ Berechtigte wird das erfasste Kennzeichen unmittelbar nach Erkennung sofort wieder gelöscht.
  - 2. Scheint das Kennzeichen nicht in der „White list“ auf, werden die Kennzeichendaten einer Weiterbearbeitung binnen einer Woche zugeführt:
- Sachbearbeiter überprüfen, ob das erfasste Kraftfahrzeug aus anderen Gründen – „nachträglich“ – zur Einfahrt berechtigt war (ggf Weiterleitung an Polizei zur weiteren Bearbeitung).
- Für die eingesetzten Verkehrsüberwachungskameras war keine besondere Rechtsgrundlage vorhanden,
- Man stützte sich auf allgemeinen Rechtsvorschriften, sodass auch für beantragte geplante automatische Verkehrsüberwachung keine ausdrückliche Rechtsgrundlage benötigt würde
- Die Zulässigkeit ergäbe sich aus den allgemeinen Vorschriften der StVO.

K600.053-023/0002-DVR/2008 SALZBURGER FUßGÄNGERZONE

- Ausführungen DSK:
  - Bei allen Fahrzeugen, die sich nicht auf der sog. „White-list“ befinden, sollen Grund und Ziel ihrer Einfahrt in die Fußgängerzone ermittelt werden, wobei es sich durchaus in vielen Fällen um berechtigte Zufahrt handeln wird, sodass die Überwachung in diesen Fällen als besonders eingriffsintensiv empfunden werden muss.
  - Massiver Eingriff in das Grundrecht auf Datenschutz vor allem jener Personen darstellen, welche rechtmäßig in die Fußgängerzone einfahren und sich erst nachträglich als dazu berechtigt herausstellen.
  - Beantragte Videoüberwachung war mangels gesetzlicher Deckung im Sinne des § 1 Abs. 2 DSG 2000 als unzulässiger Eingriff in das Grundrecht auf Datenschutz zu werten, weshalb die Registrierung der Meldung der BPD Salzburg abzulehnen war.

K600.053-023/0002-DVR/2008 Salzburger Fußgängerzone

- Ausführungen DSK:
  - jede elektronische Verarbeitung personenbezogener Daten stellt einen Eingriff in das Grundrecht auf Datenschutz dar
  - Eingriff ist, wenn er durch eine Behörde zu hoheitlichen Zwecken vorgenommen wird und nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, nur aufgrund einer besonderen gesetzlichen Ermächtigung oder Verpflichtung zulässig (§ 1 Abs. 2 DSG 2000).
  - **Antragsteller hat auf Zuständigkeit für „Verkehrspolizei“ nach § 94b StVO hingewiesen**
  - die Verwendung von Videoüberwachung zur Erfüllung einer gesetzlich übertragenen Aufgabe stellt einen so gravierenden Eingriff in das Grundrecht auf Datenschutz dar, dass der Gesetzesvorbehalt in § 1 Abs. 2 DSG 2000 … im Sinne einer spezifischen Determinierungspflicht… so zu verstehen ist, **dass ein Gesetz im formellen Sinn zum Gebrauch des Mittels „Videoüberwachung“ ausdrücklich ermächtigen muss**.

Beispiel: IT-Einsatz-Gesetz

- Das Gesetz enthält dabei Anforderungen der
  - Transparenz,
  - Beherrschbarkeit
  - Robustheit und
  - Sicherheit der Systeme.

- Bestimmte „datengetriebene Informationstechnologien“ in bestimmten Anwendungsbereichen generell unzulässig
- KI-Einsatz unzulässig, wenn Ermessen und Beurteilungsspielräume beim Erlass von Verwaltungsakten möglich sind.

Beispiel: IT-Einsatz-Gesetz

- KI-Systeme müssen verpflichtend einer der folgenden Kategorien zugeordnet werden
  - Assistenzsystem,
  - Delegation und
  - autonome Entscheidung.

- zudem (mit Einschränkungen) Offenlegungspflichten betreffend Algorithmen und weitere Transparenzpflichten
- bestimmte Verwaltungsakte bei Nichterfüllung der Erfordernisse nichtig

Beispiel: IT-Einsatz-Gesetz

- Normierung
  - der Notwendigkeit des Bestehens menschlicher Aufsicht (unter Nennung von konkreten Kontaktpersonen)
  - sowie der Vorrang menschlicher Entscheidungen
- je höher der Grad der Automation desto umfangreichere Maßnahmen zur Gewährleistung der Beherrschbarkeit der datengetriebenen Informationstechnologien
- durch KI-Rüge, können Betroffene innerhalb eines Monats ab Bekanntgabe einer KI-basierten Entscheidung verlangen, dass eine Überprüfung der Entscheidung durch eine natürliche Person erfolgt.

Beispiel: IT-Einsatz-Gesetz

- Bevor eine öffentliche Stelle KI-Systeme erstmalig
  - trainiert oder
  - einsetzt,
  - ist eine Technik-Folgenabschätzung durchzuführen
- Sofern eine Verarbeitung von personenbezogenen Daten erfolgt, ist eine Datenschutz-Folgenabschätzung durchzuführen
- Hinweis für Ausgestaltung entsprechender Rechtsgrundlage:
  - Mitgliedstaatliche Rechtsakte im Anwendungsbereich einer Verordnung sind wegen des Anwendungsvorrangs des Unionsrechts unzulässig, wenn sie die unmittelbare Geltung der Verordnung verbergen könnten
  - Auch Wiederholung des Wortlauts der Verordnung im mitgliedstaatlichen Recht ist wegen des unionsrechtlichen Wiederholungsverbotes unzulässig.

KI UND EINGRIFFE IN DAS GRUNDRECHT AUF DATENSCHUTZ

AI-Act: *…die DSGVO bleibt unberührt…*

AI-Act und DSGVO

DSGVO ist parallel zum AI-Act anzuwenden

- Art 2 Z 7 AI-Act: AI-Act berührt die DSGVO nicht, „*unbeschadet der Artikel 10 Absatz 5 und Artikel 59*“
- **Art 10 Abs 5 AI-Act** enthält Bedingungen für die Zulässigkeit der Verwendung sensibler Daten (Art 9 Abs 1 DSGVO)
  - **Anbieter** dürfen beim Trainieren, Validieren und Test von Hochrisiko-KI-Systeme „*ausnahmsweise*“ **sensible Daten verarbeiten**, um die **Erkennung und Korrektur von Bias** (Verzerrung) sicherzustellen
  - ErwGr 70: Anbieter können sich dabei auf **Art 9 Abs 2 lit g DSGVO** stützen, da dies eine „*Angelegenheit von erheblichen öffentlichen Interesse*“ ist
- **Art 59 AI-Act** enthält Bedingungen für die (Weiter)Verarbeitung pbD zur Entwicklung, Training und Testen bestimmter KI-Systeme im **KI-Reallabor** (Sandbox)
  - ErwGr 140: **Anbieter** dürfen **pbD verarbeiten** im Rahmen der Entwicklung bestimmter KI-System innerhalb eines KI-Reallabors, basierend auf **Art 6 Abs 4 bzw 9 Abs 2 lit g DSGVO**, zumal die Verarbeitung im erheblichen öffentlichen Interesse liegt
- **ErwGr 140 AI-Act und Art 22 DSGVO → AI-Act ist keine Rechtsgrundlage** zur **Legitimierung automatisierter Entscheidungen im Einzelfall**

DATENSCHUTZRECHT UND KI

- Datenschutzrechtliche Erfordernisse spielen eine entscheidende Rolle bei der Umsetzung von KI-Projekten wenn pb Daten verarbeitet werden
- Klärung der **datenschutzrechtlichen Rollen** (wer ist verantwortlich, besteht eine gemeinsame Verantwortlichkeit, gibt es ein AV-Verhältnis?)
- Herausforderung der Einhaltung der **datenschutzrechtlichen Grundsätze** (insb Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenrichtigkeit..)
- Informierte Einwilligung möglich? Berechtigte Interessen?
- Sicherstellung der **Betroffenenrechte**?
- Im Idealfall soweit möglich Anonymisierung der Trainingsdaten bereits während der Aufbereitung
- Prüfung ob **automatisierte Entscheidung im Einzelfall** vorliegt
- Prüfung ob **Datenschutz-Folgenabschätzung** erforderlich ist

Next Steps

- **Ordnen Sie ihr Verwaltungshandeln ein** - Hoheitsverwaltung oder Privatwirtschaftsverwaltung?
- **Eruierung einer ausreichenden Rechtsgrundlage**
  - Beim Einsatz von KI gewinnt die gesetzliche Grundlage aufgrund der verringerten personellen Legitimation an Bedeutung
- **Erfolgen Grundrechtseingriffe** im Rahmen ihrer **KI-Nutzung**?
  - Ist die Verarbeitung personenbezogener Daten Teil ihrer KI-Nutzung?
  - Beim Einsatz von KI gewinnt die gesetzliche Grundlage aufgrund der verringerten personellen Legitimation an Bedeutung
- Erstellen Sie **klare Vorgaben für Verfahrensaufgaben**
  - Was darf das KI-System machen, was dürfen User mit KI-System machen, welche Daten dürfen und dürfen nicht eingegeben werden …
- **Informieren** Sie betroffene Person **vorab über den Einsatz von KI**
- Führen Sie eine **Datenschutz-Folgenabschätzung** (DSFA) durch

Näheres erfahren Sie hier → Publikation: Einsatz von KI in der Verwaltung – Anforderungen aus den Blickwinkeln des Legalitätsprinzips und des Datenschutzrechts, Digitalisierung und Recht 2024, *Scheichenbauer*, *Rothmund-Burgwall* (September 2024)

Danke für Ihre Aufmerksamkeit!

Dr. Heidi Scheichenbauer
heidi.scheichenbauer@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Florianigasse 55/10, 1080 Wien
www.researchinstitute.at

RECHTLICHE HINWEISE

Zweck: Dieses Dokument dient als Trainingsunterlage.

Erstellt von: Dr. Heidi Scheichenbauer

Copyright:

Disclaimer:

Dieses Dokument wurde auf Basis jener Informationen erstellt, die dem Autor als für den Zweck des Dokuments relevant erschien. Der Autor übernimmt jedoch keine Haftung/Gewähr für Vollständigkeit und Richtigkeit der in diesem Dokument zur Verfügung gestellten Informationen. Die Angaben in diesem Dokument können von dem Empfänger nicht als Zusicherung oder Garantie verstanden werden. Die in diesem Doku ment enthaltenen Informationen können sich im Laufe der Zeit verändern oder zum Übergabezeitpunkt bereits verändert haben. Technische Änderungen vorbehalten.

Kontaktdaten: heidi.scheichenbauer@researchinstitute.at