aringer herbst winklbauer

AI ACT UND DSGVO – BEZIEHUNGSSTATUS: ES IST KOMPLIZIERT

12. Oktober 2025
LSZ CIO Kongress

Mag. Constantin Maetz
Rechtsanwaltsanwärter

AGENDA

1. INTRO: Definitionen der KI-VO
2. Anwendbarkeit der DSGVO
3. Rechtmäßigkeit der Verarbeitung personenbezogener Daten
4. Anonymität eines KI-Modells

Wrap up & Discussion

KI-SYSTEM

*„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. **Computer-programm (Software)**

2. **Erzeugt Ergebnisse durch Ableitung von Eingaben**

3. **relevante Information für Empfänger**

4. **gewisse Autonomie**

→ KI-System verwendet keine einfachen herkömmlichen Programmieransätze

KI-MODELL

ErwGr 97: *„Obwohl KI-Modelle wesentliche Komponenten von KI-Systemen sind, stellen sie für sich genommen keine KI-Systeme dar. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon“*

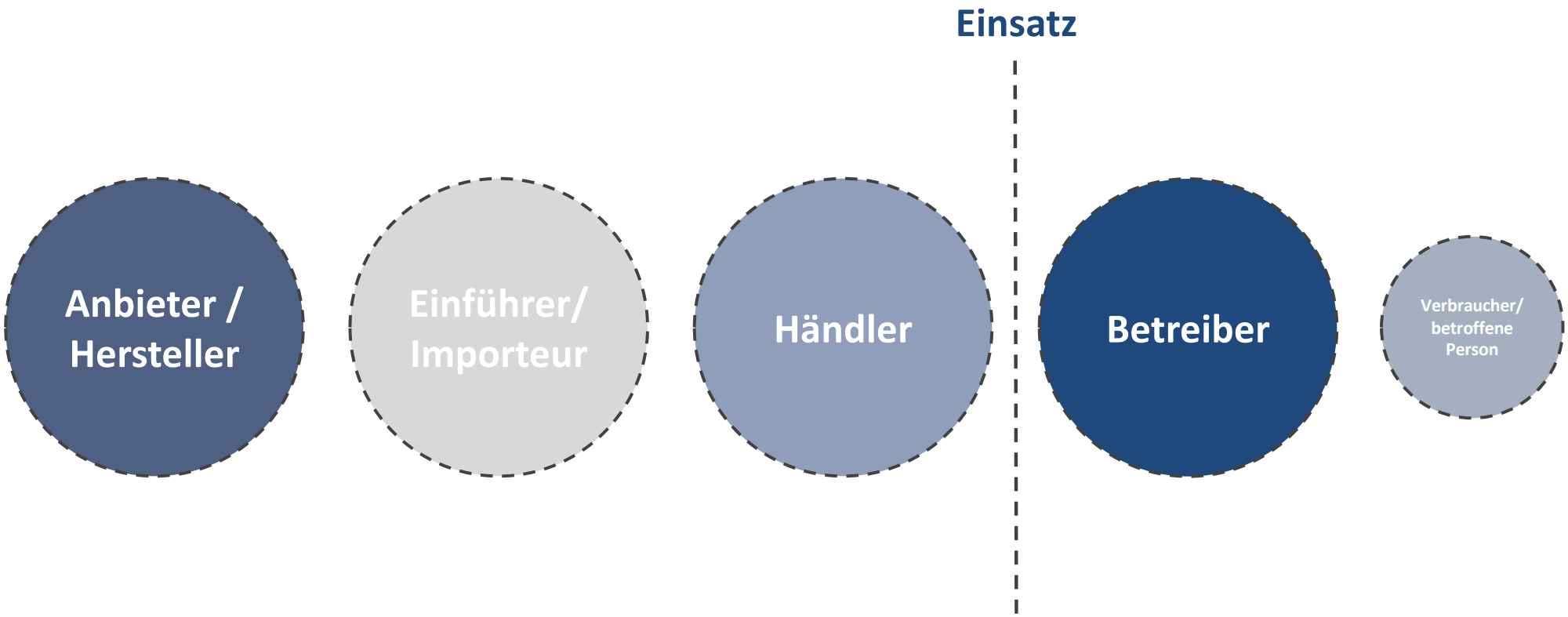
1. mit **großer Datenmenge** trainiert

2. **Ergebnis verschiedener Trainingsmethoden**

3. **keine Nutzerschnittstelle**

→ KI-Modell ist idR ein wesentlicher Bestandteil eines KI-Systems

„AKTEURE“ (WHO IS WHO?)



AGENDA

1. INTRO: Definitionen der KI-VO
2. Anwendbarkeit der DSGVO
3. Rechtmäßigkeit der Verarbeitung personenbezogener Daten
4. Anonymität eines KI-Modells

Wrap up & Discussion

LEBENSZYKLUS EINES KI-MODELLS

Verarbeitung personenbezogener Daten

KI-Modell

Entwicklungsphase

- **Trainingsdaten** enthalten personenbezogene Daten
- Rechtmäßigkeit der Verarbeitung pb Daten zum Trainieren einer KI
- Maßnahmen zur Verhinderung der Verarbeitung pb Daten beim Training (Anonymisierung / Pseudonymisierung, Filterung …)

Einsatzphase

- **Input-/Outputdaten** enthalten personenbezogene Daten
- Rechtmäßigkeit der Verarbeitung pb Daten
- Verarbeitung pb Daten vom Zweck des Systems umfasst
- Technische/organisatorische Maßnahmen zur Verhinderung der Verarbeitung pb Daten beim Einsatz
- Weiterverarbeitung zu Trainingszwecken?

→ Unterschiedliche Überlegungen je nach Lebensphase des KI-Modells

KI-VO UND DSGVO

Art 2 Abs 7 KI-VO: Die DSGVO bleibt unberührt

2 Ausnahmen (Öffnungsklauseln):

1.

Art 10 Abs 5 KI-VO iVm Art 9 Abs 2 lit g DSGVO

Verarbeitung sensibler Daten zur **Erkennung und Korrektur von Verzerrungen** in einem KI-Modell

(zB Gendermedizin, Biasfreiheit …)

2.

Art 59 Abs 1 KI-VO iVm Art 6 Abs 4 DSGVO

Weiterverwendung personenbezogener Daten zu einem anderen Zweck als zu dem sie erhoben wurden **in KI-Reallaboren**

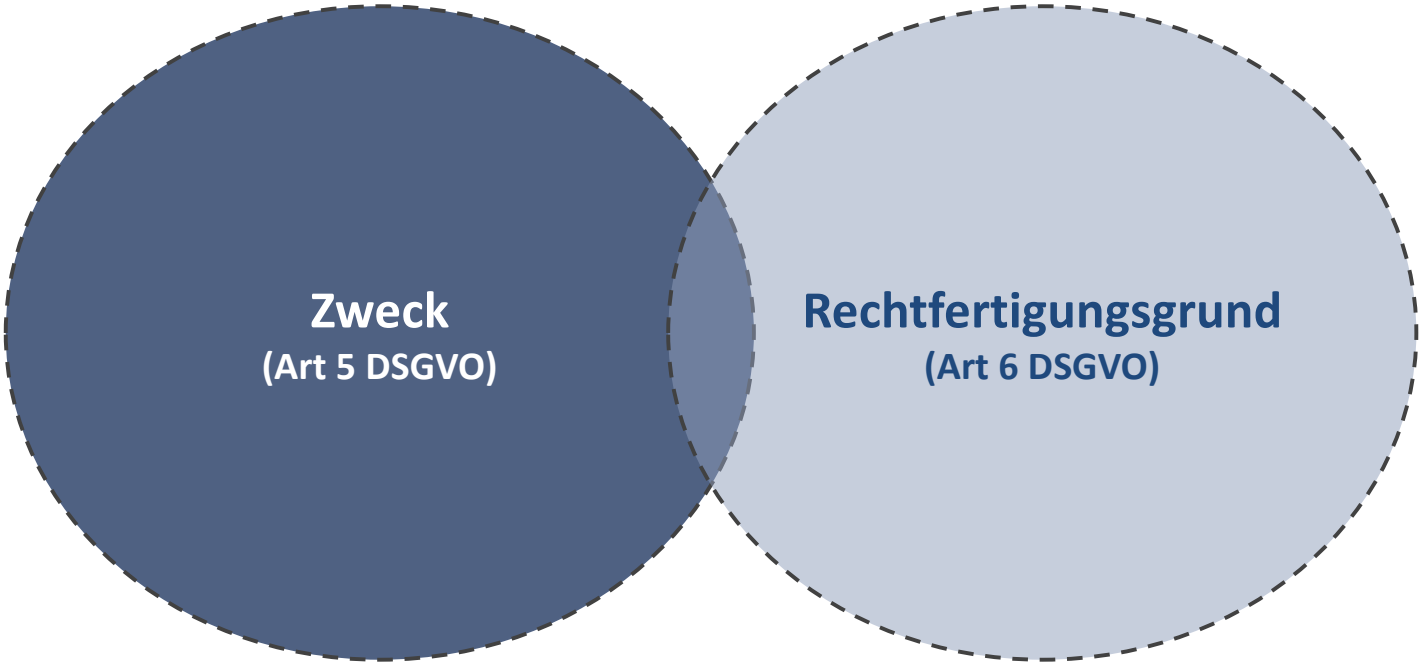
→ Die KI-VO bietet grundsätzlich keinen Rechtfertigungsgrund (2 Ausnahmen)

AGENDA

1. INTRO: Definitionen der KI-VO
2. Anwendbarkeit der DSGVO
3. Rechtmäßigkeit der Verarbeitung personenbezogener Daten
4. Anonymität eines KI-Modells

Wrap up & Discussion

RECHTMÄßIGE VERARBEITUNG PB DATEN



→ Verantwortlicher hat Zweck und Rechtfertigungsgrund festzulegen und darüber zu informieren

RECHTMÄßIGE VERARBEITUNG PB DATEN FÜR / DURCH KI

Datenschutzrechtliche Grundprinzipien

Zweckbindung

Entwicklung

- Training eines KI-Modells
- Bestimmung eines Anwendungsbereichs
- nicht alle Use-Cases mögl.
- ggf. Negativabgrenzung

Einsatz

- Einsatz für bestimmte/n Anwendungsfall/-fälle (technischer Support, Buchhaltung, HR, …)
- Weiterverarbeitung nur bei Zusammenhang & Vereinbarkeit (Entwicklung)

Rechtfertigungsgrund

Entwicklung

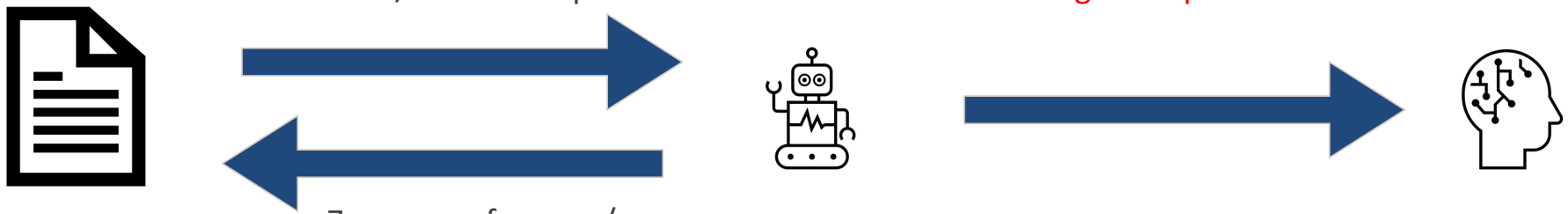
- Einwilligung
- Berechtigtes Interesse der Entwicklung eines sicheren Systems
- Sicherstellung hoher Datenqualität
- Bias-Freiheit, Verzerrung

Einsatz

- Vertragserfüllung (zB technischer Support)
- Einwilligung
- Berechtigtes Interesse Effizienzsteigerung, Kostenersparnis, …

→ keine Weiterverarbeitung pb Daten zu einem anderen Zweck (selbstlernende Systeme)

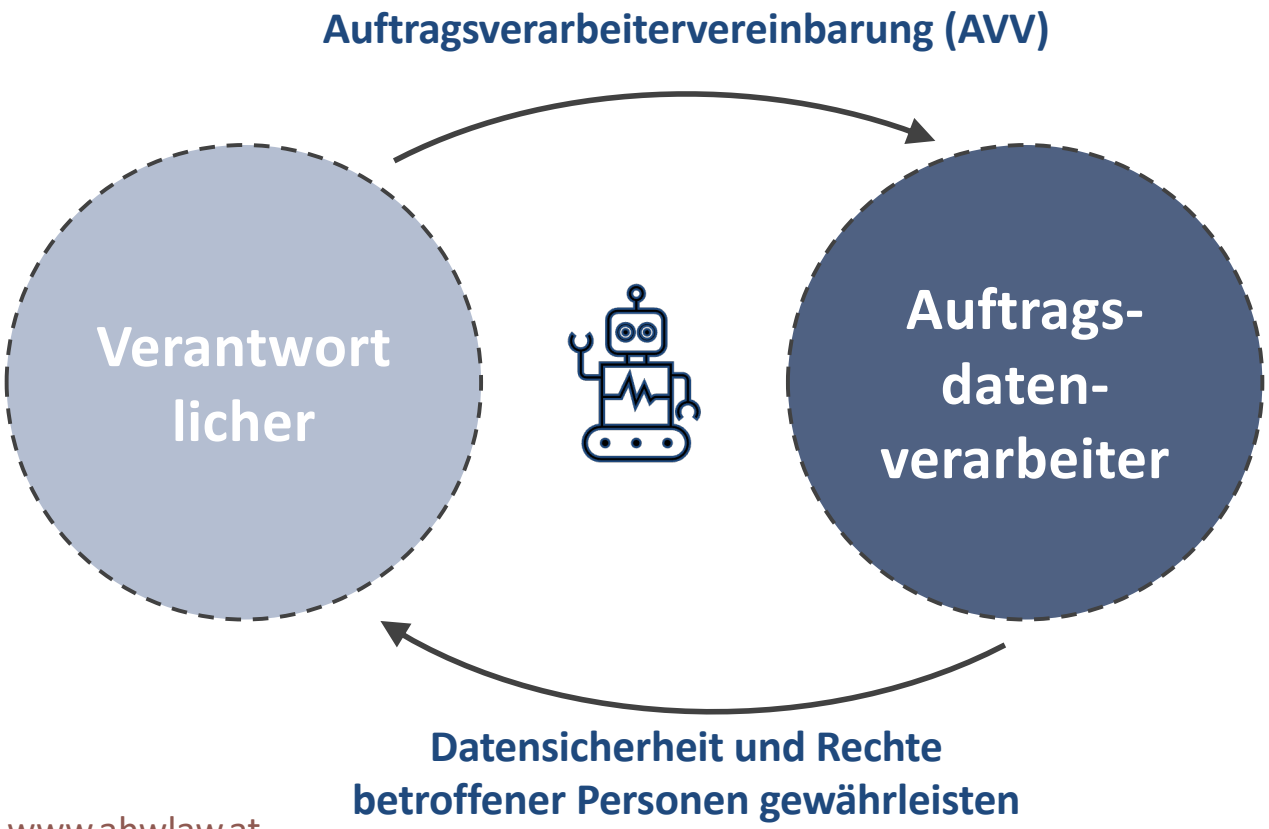
EINSATZ UND WEITERVERARBEITUNG



✓ **Verarbeitung 1:** Zusammenfassung eines Dokuments / Kategorisierung von E-Mails

✗ **Verarbeitung 2:** Training der KI mit personenbezogenen Daten und Inhalten des Dokuments / der E-Mails

DATENTRANSFER (BEIM EINSATZ VON KI-SYSTEMEN)



Datentransfer i.O., wenn:

- **AVV** zur Gewährleistung von Datensicherheit und Rechten betroffener Personen
- technisch organisatorische Maßnahmen zum Schutz pb Daten
- ggf. **SCC** beim **Drittlandsdatentransfer** ohne Angemessenheitsbeschluss
- Haftung des Verantwortlichen bei **Kontrollverlust**
- Training mit Inputdaten führt zu Kontrollverlust über personenbezogene Daten

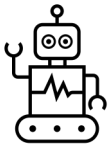
RECHTE BETROFFENER PERSONEN

Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung, Ergänzung, Löschung**
- Recht auf **Widerspruch** (bei Einwilligung)
- Recht auf **Übertragung** (Kopie der Daten)
- Recht auf **Beschwerde**
- Recht keiner **automatisierten Entscheidung** zu unterliegen

Wann ist der österreichische Bundespräsident geboren?

Der österreichische Bundespräsident ist am 1.1.2020 geboren.



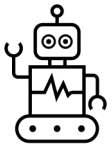
RECHTE BETROFFENER PERSONEN

Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung, Ergänzung, Löschung**
- Recht auf **Widerspruch** (bei Einwilligung)
- Recht auf **Übertragung** (Kopie der Daten)
- Recht auf **Beschwerde**
- Recht keiner **automatisierten Entscheidung** zu unterliegen

Wann ist der österreichische Bundespräsident geboren?

Ich kann leider keine spezifischen Angaben zu personenbezogenen Daten machen.



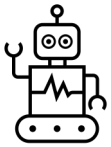
RECHTE BETROFFENER PERSONEN

Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung, Ergänzung, Löschung**
- Recht auf **Widerspruch** (bei Einwilligung)
- Recht auf **Übertragung** (Kopie der Daten)
- Recht auf **Beschwerde**
- Recht keiner **automatisierten Entscheidung** zu unterliegen

Welchen Bewerber sollen wir einstellen?

Stellen Sie Bewerber X ein, Bewerber Y ist nicht qualifiziert.



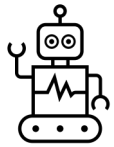
RECHTE BETROFFENER PERSONEN

Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung, Ergänzung, Löschung**
- Recht auf **Widerspruch** (bei Einwilligung)
- Recht auf **Übertragung** (Kopie der Daten)
- Recht auf **Beschwerde**
- Recht keiner **automatisierten Entscheidung** zu unterliegen

Welchen Bewerber sollen wir einstellen?

Ich kann leider keine Personalentscheidungen treffen. Bewerber X hat rein formal die besseren Qualifikationen.



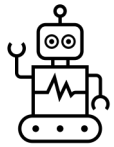
RECHTE BETROFFENER PERSONEN

Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung, Ergänzung, Löschung**
- Recht auf **Widerspruch** (bei Einwilligung)
- Recht auf **Übertragung** (Kopie der Daten)
- Recht auf **Beschwerde**
- Recht keiner **automatisierten Entscheidung** zu unterliegen

Bin ich kreditwürdig?

Nein, Sie können keinen Kredit bekommen. Ihr Antrag wird abgelehnt.



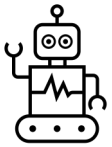
RECHTE BETROFFENER PERSONEN

Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung, Ergänzung, Löschung**
- Recht auf **Widerspruch** (bei Einwilligung)
- Recht auf **Übertragung** (Kopie der Daten)
- Recht auf **Beschwerde**
- Recht keiner **automatisierten Entscheidung** zu unterliegen

Bin ich kreditwürdig?

Die Bewertung ihrer Kreditwürdigkeit erfolgt durch einen Mitarbeiter.



AGENDA

1. INTRO: Definitionen der KI-VO
2. Anwendbarkeit der DSGVO
3. Rechtmäßigkeit der Verarbeitung personenbezogener Daten
4. Anonymität eines KI-Modells

Wrap up & Discussion

ANONYMITÄT EINES KI-MODELLS

- **praktisch unmöglich** personenbezogene Daten aus Trainingsdaten zu erhalten (durch statistische „Tricks“ wie zB Membership Interference, Regurgitation, Model Inversion)
- „**Vernachlässigbar geringe Chance**“ durch vorsätzliche oder zufällige Anfragen personenbezogene Daten zu erlangen

1. Unmöglichkeit

personenbezogene Daten aus dem Datensatz herauszufiltern

2. Prüfung

aller **Mittel, die „vernünftigerweise eingesetzt werden könnten**“, um natürliche Personen zu identifizieren (ErwGr 26 DSGVO)

3. Risikobewertung

ob Identifizierung durch Verantwortliche oder Dritte möglich ist, die sich Zugriff auf den betreffenden Datensatz verschaffen könnten

MAßNAHMEN ZUR ERREICHUNG VON ANONYMITÄT

GESTALTUNG DES MODELLS

- **Quellen** ohne personenbezogene Daten
- **Datenaufbereitung** und –minimierung (Anonymisierung / Pseudonymisierung, Datenfilterungsprozesse …)
- **Methodenauswahl** zur Verhinderung/Reduzierung einer Identifikation (**Differential Privacy** – „statistisches Rauschen“)
- Vorkehrungen bei der Ausgabe (Ausgabefilter)

PRÜFUNG DES MODELLS

- gezielte Tests zur Prüfung der Angriffsresistenz
  - Attribute und Membership Inference
  - Exfiltration
  - Regurgitation
  - Model Inversion
  - Reconstruction Attacks
- Dokumentation (Nachweis der Resistenz)
- Bewertung von Folgerisiken (Datenschutzfolgenabschätzung / Grundrechtliche Folgenabschätzung für Hochrisiko-KI)

→ Anonymität des KI-Modells garantiert nicht Anonymität beim Einsatz!

KEY TAKE-AWAYS UND Q&A

1. **Trennung** zwischen **Entwicklung** und **Einsatz** hinsichtlich der Rechtmäßigkeit der Verarbeitung personenbezogener Daten

2. Beachtung der **Zweckbindung** und Vorsicht beim Einsatz selbstlernender Systeme

3. **Keine Weiterverarbeitung** durch Training aus personenbezogenen Inputdaten
→ Kontrollverlust

4. **Anonymität** des Modells schließt nicht Anwendbarkeit der DSGVO beim Einsatz aus

→ Diskussion und Fragen

VIELEN DANK!

Mag. Constantin Maetz
Rechtsanwaltsanwärter

aringer herbst winklbauer rechtsanwälte

Grillparzerstraße 5, 1010 Wien
+43 1 890 90 17
maetz@ahwlaw.at