Deutsche Stiftung für Recht und Informatik

Update Datenschutz

Dr. Flemming Moos
Osborne Clarke

Update Datenschutz

1. Zwecksetzungsfreiheit und Datenminimierung
2. Vermeidung einer Unternehmenshaftung für Datenschutzverstöße
3. Personenbezug von KI-Modellen

1. Zwecksetzungsfreiheit und Datenminimierung (1)

- Vereinzelte Positionen zur Datenminimierung:
  - LfDI Bremen: Die Erhebung einer E-Mail-Adresse im Online-Versandhandel zwecks Zustellung einer Bestellbestätigung ist unzulässig, weil diese auch zum Download im Internet vorgehalten werden könne.
  - LG München: Die Übertragung einer IP-Adresse an den Anbieter einer Schriftart ist nicht nach Art. 6 Abs. 1 DSGVO zu rechtfertigen, weil eine Schriftart auch auf einem eigenen Server gehostet werden könne.
  - DSK: Einem Online-Shops ist es untersagt, Waren nur an registrierte Nutzer / Inhaber eines Kunden-kontos zu verkaufen.
- Nach dieser Logik gälte auch das…
  - Ein Online-Händler dürfte nicht mehr verpflichtend eine Lieferung an die Adresse des Bestellers vornehmen, weil unter Verzicht auf die Erhebung von Adressdaten eine Auslieferung an Packstationen erfolgen kann.
  - Ein Händler dürfte im stationären Handel nicht die Bezahlung mittels EC-Karte vorsehen, weil sie im Vergleich zur Barzahlung mit einem Mehr an Datenverarbeitung einhergeht.
  - Ein Rechtsanwalt müsste sich fragen, ob er eine Klage unter verpflichtender Angabe personenbezogener Daten (z.B. von Zeugen) überhaupt erheben dürfte, weil es ggf. datensparsamere Möglichkeiten der Rechtsverfolgung gäbe…

1. Zwecksetzungsfreiheit und Datenminimierung (2)

- Höchstrichterliche Klarstellung durch Entscheidung des BVerwG vom 20. März 2024
  - Entscheidung zur Frage, ob zwecks Bearbeitung eines IFG-Antrags vom Antragsteller die Angabe seiner Anschrift verlangt werden könne
  - BVerwG bejaht Erforderlichkeit im Einklang mit Datenminimierungsgrundsatz:

    „„[…] *die anhand der Anforderungen des Fachrechts getroffenen Zweckfestsetzungen sind der DSGVO vorgelagert und werden von dieser Verordnung nicht wieder hinterfragt. Vielmehr bilden sie den Ausgangspunkt der rechtlichen Überprüfung nach den Maßgaben des durch die Verordnung statuierten Zweckbindungsgebots. Der Grundsatz der Datenminimierung setzt eine dem Art. 5 Abs. 1 Buchst. b DSGVO genügende Zweckbestimmung voraus und knüpft seine Erfordernisse hieran an, nicht umgekehrt.“*
  - Behörde durfte den Zweck der ordnungsgemäßen Bearbeitung des IFG-Antrags festgelegen, für die eine Identifizierung des Antragstellers erforderlich war.

1. Zwecksetzungsfreiheit und Datenminimierung (3)

- Bewertung und rechtliche Einordnung
  - Gleichlauf mit sonst. Entscheidungen
    - OLG München: Grundsatz der Datenminimierung steht verpflichtender Angabe des Klarnamens bei der Anmeldung zu einem sozialen Netzwerk nicht entgegen.
    - VG Lüneburg: Bei Beurteilung der Erforderlichkeit ist in Rechnung zu stellen, dass dem Arbeitgeber die nach Art. 12 GG verbriefte unternehmerische Entscheidungs-freiheit zusteht, wie er seinen Betrieb organisiert.
    - LG Passau: Kein Anspruch darauf, dass Facebook dergestalt betrieben wird, dass sämtliche Daten in Europa verarbeitet werden. Die unternehmerische Entscheidung, Daten in den USA zu verarbeiten, ist hinzunehmen.
  - Konsequenzen
    - Grundsatz der Datenminimierung bezieht sich nur auf die Datenverarbeitung und verlangt deshalb nicht nach einer absoluten Reduzierung oder Beschränkung der Datenmenge
    - Verantwortlicher hat bei Auswahl der Zwecke und Festlegung der Verarbei-tungsmittel Beurteilungsspielraum
    - diesen nutzt er datenschutzkonform aus, wenn die gewählte Vor-gehensweise geeignet und angemessen ist, den verfolgten Zweck zu erfüllen.

2. Vermeidung von Unternehmenshaftung für Datenschutzverstöße (1)

- Ausgangslage auf Basis bisheriger EuGH- (und Instanz-) Rechtsprechung
  - insgesamt eher geringe Anforderungen an das Vorliegen eines Schadens i.S.v. Art. 82 DSGVO, z.B.:
    - Keine Erheblichkeitsschwelle / Bagatellgrenze
    - Angst vor Datenmissbrauch kann immateriellen Schaden darstellen
  - Im Unternehmensalltag werden Verstöße im Grunde immer von Beschäftigten verursacht
  - Frage: Ob und unter welchen Voraussetzungen ist ein Unternehmen (als datenschutzrechtlich Verantwortlicher) ersatzpflichtig für Schäden, die auf einem DSGVO-Verstoß beruhen, der durch einen Beschäftigten begangen wurde?

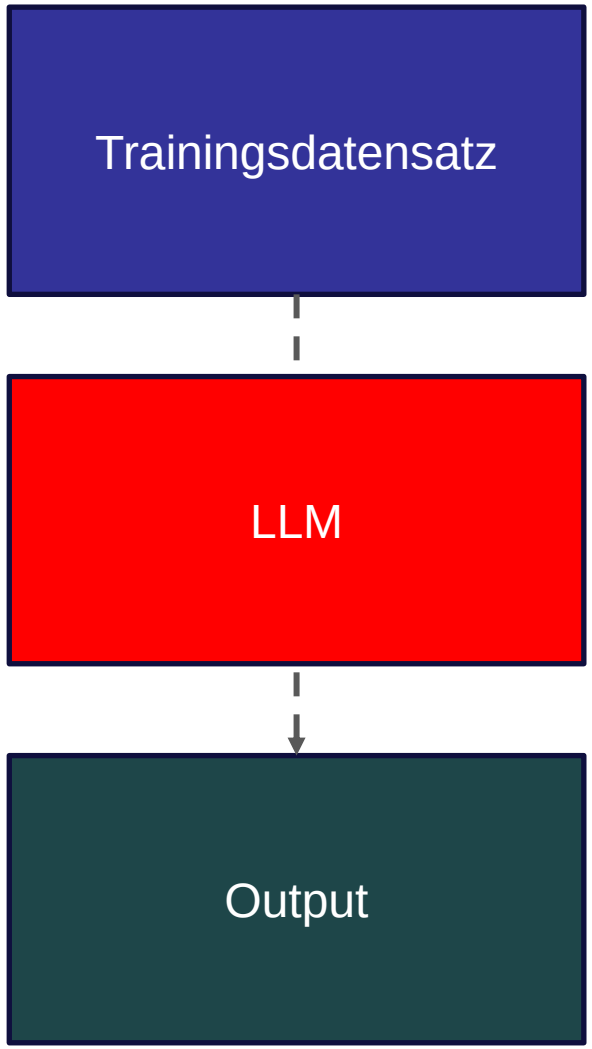
2. Vermeidung von Unternehmenshaftung für Datenschutzverstöße (2)

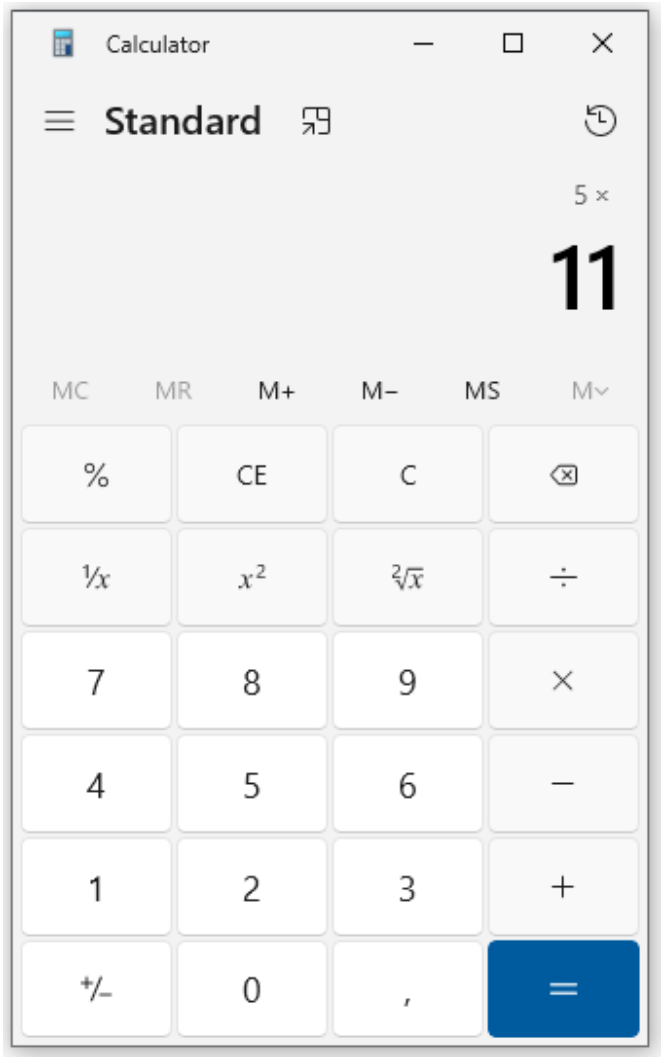
- Urteil des EuGH vom 11. April 2024 in Sachen *juris*
  - Gericht legt strenges Verständnis an das Verschuldenserfordernis an und bejaht im Ergebnis eine Einstandspflicht des Unternehmens
  - Haftung aus vermutetem Verschulden: Beweislast des Verantwortlichen, dass kein Verschulden vorliegt (Art. 82 Abs. 2 und 3 DSGVO)
  - Exkulpation nur unter engen Voraussetzungen möglich: Verantwortlicher muss nachweisen, dass er selbst nicht für den Schaden verantwortlich ist
  - Im Falle einer von einem Beschäftigen ausgelösten Datenpanne: Nachweis, dass kein Kausalzusammenhang zwischen der Verletzung der Art. 5, 24 und 32 DSGVO und dem Schaden besteht
  - Für eine Haftungsbefreiung nicht ausreichend, dass Verantwortlicher nachweist, den unterstellten Personen Weisungen gen. Art. 29 DSGVO erteilt zu haben und eine Person weisungswidrig gehandelt hat

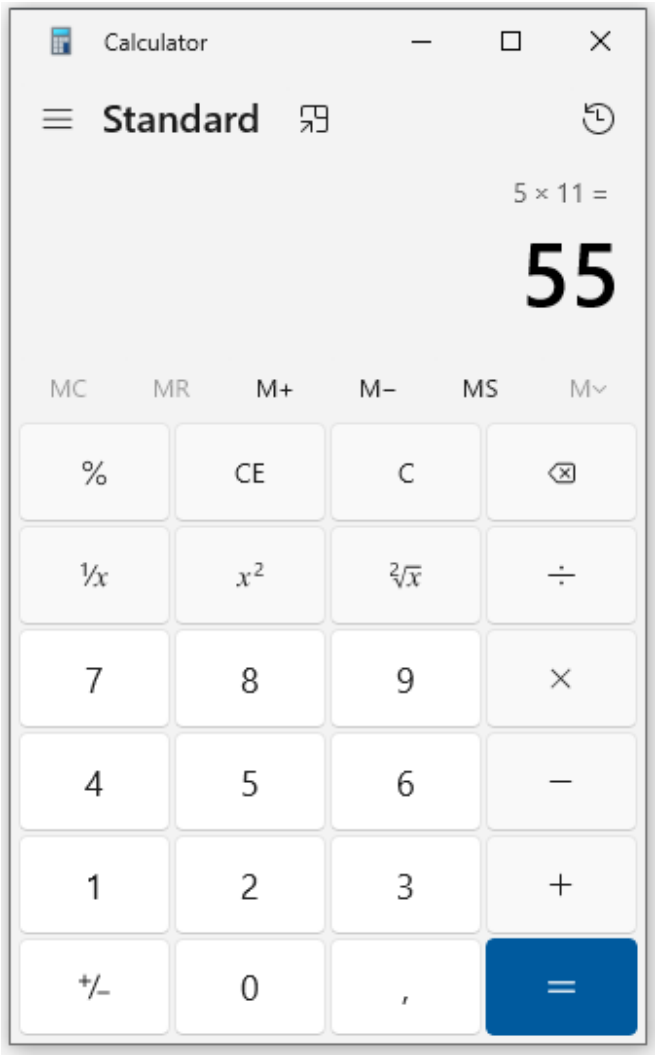
2. Vermeidung von Unternehmenshaftung für Datenschutzverstöße (3)

- Bewertung und rechtliche Einordnung
  - Im Ausgangspunkt keine (unmittelbare) Zurechnung des individuellen durch den Arbeitnehmer begangenen Verstoßes
  - Es scheint dem EuGH auf ein (eigenes) Organisationsverschulden des Unternehmens anzukommen
  - Nur vage Andeutungen, welche Voraussetzungen für Exkulpation erfüllt sein müssen:
    - einmalige, allgemeine Weisung des Mitarbeiters nicht ausreichend
    - Jedenfalls unzureichend in der Form von Prozessbeschreibung
    - Verantwortlicher muss sich vergewissern, dass seine Weisungen von seinen Arbeitnehmern korrekt ausgeführt werden
    - die Einhaltung solcher Weisungen sollten (mindestens stichprobenartig) Gegenstand interner Datenschutzaudits sein

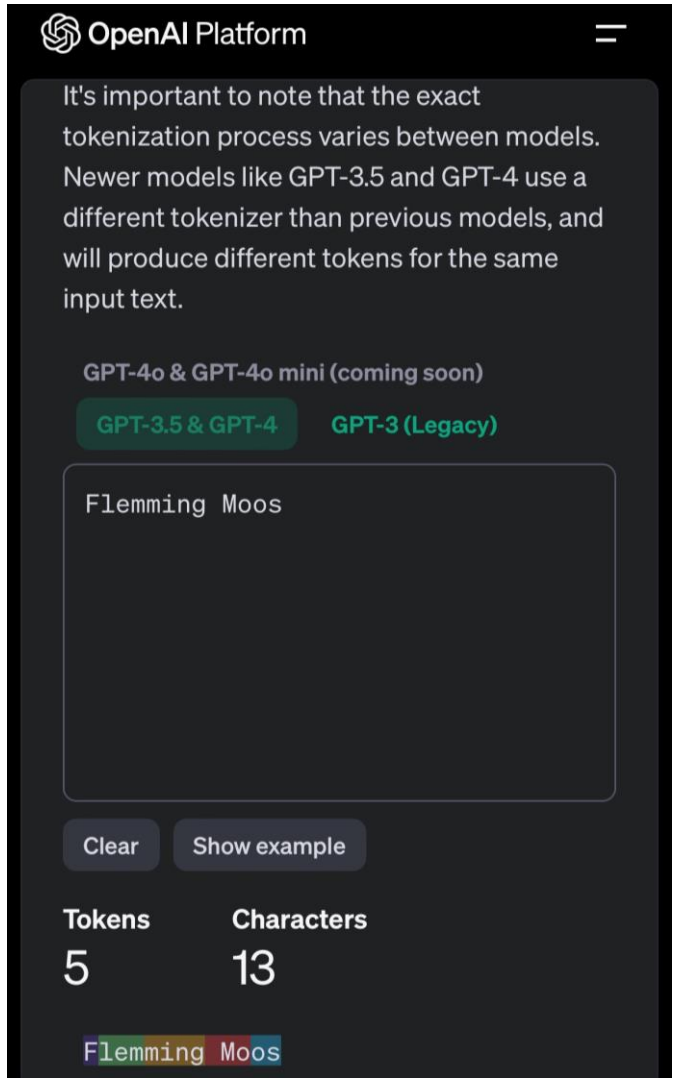
3. Personenbezug von KI-Modellen (1)

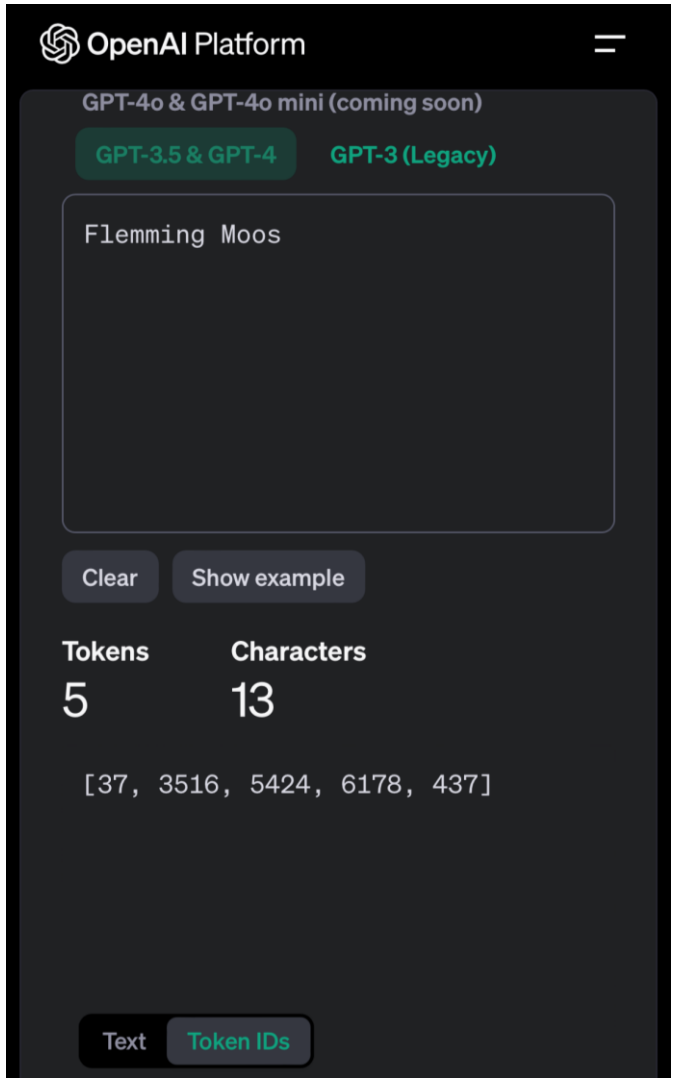






Personenbezug von KI-Modellen (2)





Tokenisierung:

Flemming Moos

[F][lem][ming][Mo][os]

[37, 3516, 5424, 6178, 437]

In dieser Form Ausgangsbasis für Embedding, bei dem Token als abstrakte Wahrscheinlichkeit einer Buchstaben- und Zahlenfolge in den vieldimensionalen Vektorraum des LLM eingebettet werden:

[0.25 -0.12 2.78 …. 0.42]

3. Personenbezug von KI-Modellen (3)

- offen:
  - LfDI BW: Personenbezug von KI-Modellen könne sich daraus ergeben, „*dass im KI-Modell die personenbezogenen Daten selbst enthalten*“ seien.
  - BayLDA: Punkt in der Checkliste, „*ob ein erstelltes KI-Modell an sich einen Personenbezug aufweist oder nicht*“.
- eindeutig:
  - **Datatilsynet** – Stellungnahme vom 19. Januar 2024 (unter Berufung auf Leitfaden aus Okt. 2023): *Die dänische Datenschutzbehörde geht davon aus, dass ein KI-Modell im Ausgangspunkt selbst kein personenbezogenes Datum darstellt, sondern nur das Ergebnis der Verarbeitung personenbezogener Daten ist. Dies entspricht der Einstufung eines statistischen Berichts, der ebenfalls nicht als personenbezogenes Datum gilt, wenn der Bericht nur Schlussfolgerungen und aggregierte Daten enthält, die das Ergebnis der statistischen Analyse sind.*“
  - **HmbBfDI** - Diskussionspapier: Large Language Models und personenbezogene Daten vom 15. Juli 2024: „*Die bloße Speicherung eines LLMs stellt keine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar. Denn in LLMs werden keine personenbezogenen Daten gespeichert*.“

3. Personenbezug von KI-Modellen (4)

- Wesentliche Argumente gegen einen Personenbezug
  - Daten zu identifizierter Person (-), unstreitig keine Identifikatoren als „Klardaten“ enthalten
  - Daten zu identifizierbarer Person?
    - Keine Identifikation durch Prompting („Memorisieren“ von Trainingsdaten), dies bewirkt „Neuschaffung“ der Daten („Rekonstruktion“) anhand der im Training erlernten Regeln.
    - Identifikation verlangt eindeutige und objektive Zuordnung zu einer Person, die hier nicht gegeben ist (Halluzinationen). Bezugsperson der Daten ist in dem Modell selbst nicht mit der notwendigen Eindeutigkeit festgelegt.
    - Keine Identifikation durch Model Attacks; wiederum keine hinreichend „sichere“ Identifikation.
    - Zudem keine Mittel, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine natürliche Person zu identifizieren; wegen Charakters der LLMs als „Blackbox“ fehlen häufig die Kenntnisse über Funktionsweise für effektive Attack-Prompts; als missbräuchliche Nutzung auch von den Modell-Entwicklern vertraglich untersagt

Vielen Dank für die Aufmerksamkeit
AM SAMSTAGMITTAG!

Bis zur nächsten HA 2025

RA Dr. Flemming Moos
Osborne Clarke, Hamburg
flemming.moos@osborneclarke.com