part of
#diwokiel24
11.- 17. Mai

Lernt KI noch Datenschutz?

Vortrag am 17. Mai 2024

Angelika Martin/Benjamin Walczak
0431 988-1200
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Übersicht

- Einführung:
  Verständnisse von Künstlicher Intelligenz
- Vier neue Thesen zu KI
- Fazit, Ausblick und Diskussion

Verständnisse von Künstlicher Intelligenz

- Was macht ein KI-System?
  - Texte + Bilder
    - Chatbots /
      Large Language Models (LLM)
    - Bildgeneratoren /
      Generative Adversial Networks (GAN)
  - Fahrzeuge fahren
  - Strukturen erkennen
    z.B. Medizinische Diagnosesysteme, Gesichtserkennung
  - ...

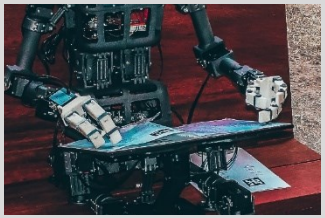

Foto von Andrea De Santis auf Unsplash

Verständnisse von Künstlicher Intelligenz

- Wie sehen wir KI-Systeme?
  - „Die KI ist dem Menschen (schon bald) überlegen.“
  - „Die KI ist (nur) ein stochastischer Papagei.“
  - „Die KI trifft (bessere) Entscheidungen.“

Foto von Andrea De Santis auf Unsplash

Verständnisse von Künstlicher Intelligenz

- Was machen wir mit KI-Systemen?
  - Vertrauen wir den Ergebnissen von KI-Systemen?
  - Wer ist Nutzer*in, wer ist das Werkzeug?
  - Wer ist verantwortlich?

Foto von Andrea De Santis auf Unsplash

Neue Thesen zu KI

- „KI ist ein Daten-Dschungel“
  - Was passiert mit den eingegebenen Daten?
    - Was und wie wird gefiltert?
    - Weitere Nutzung für KI-Training?

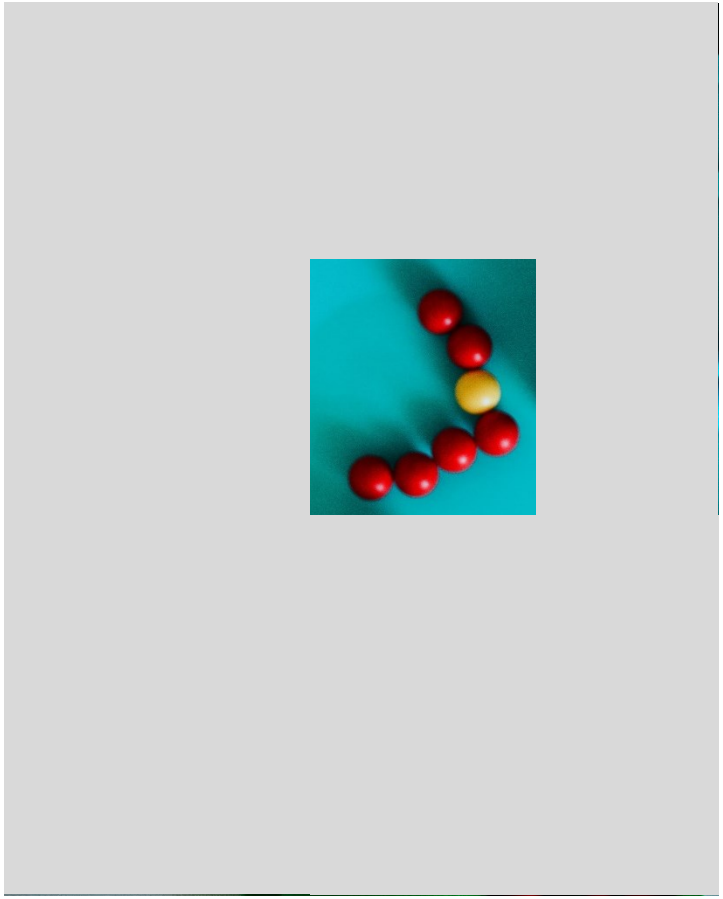

Foto von Nathan Dumlao auf Unsplash

Neue Thesen zu KI

- „KI ist ein Daten-Dschungel“
  - Wer erlangt Kenntnis von den Ein- und Ausgabedaten?
    - Nutzung für KI-Training?
    - Können Daten mit geschickten Befehlen geborgen werden?
    - Sind Ausgaben öffentlich?

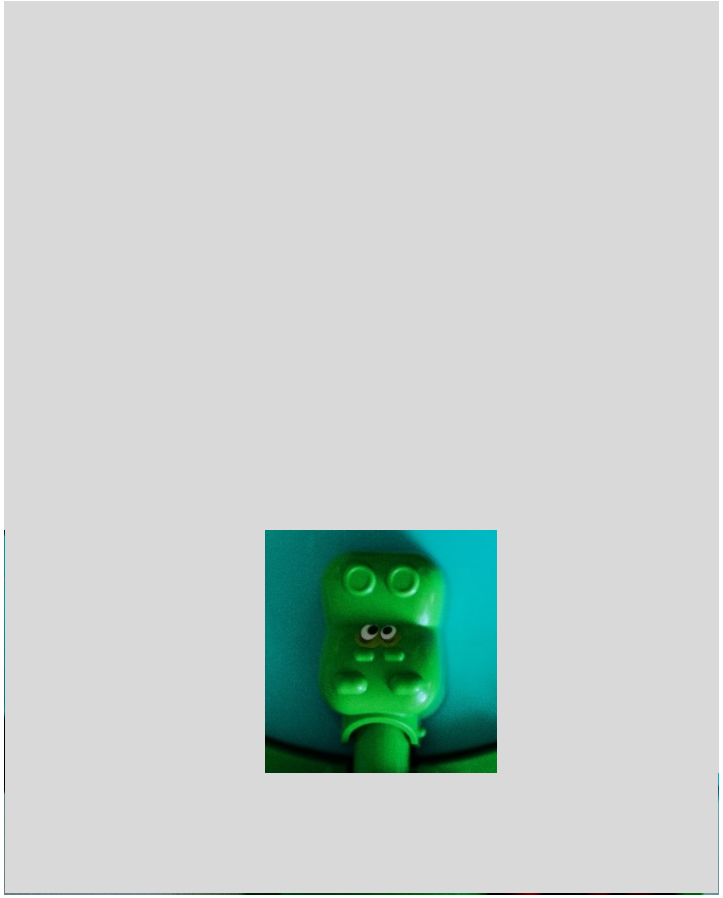

Foto von Nathan Dumlao auf Unsplash

Neue Thesen zu KI

- „KI ist ein Daten-Dschungel“
  - Wie geht man mit den Ausgaben um?
    - Prüfung der Ergebnisse?
    - Weitere Nutzung für KI-Training?

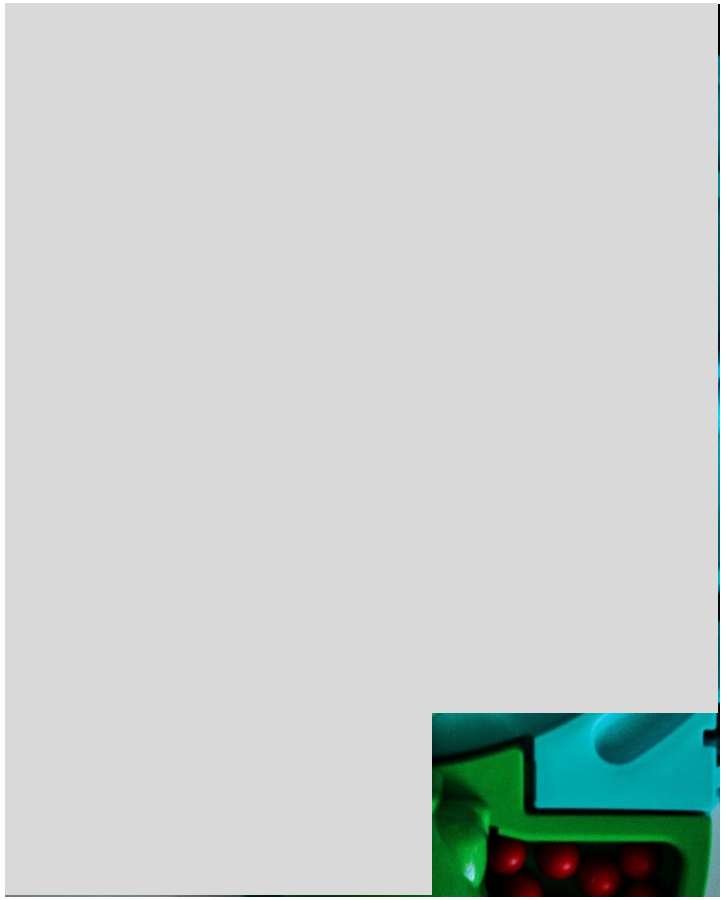

Foto von Nathan Dumlao auf Unsplash

Neue Thesen zu KI

Eingabe / Ausgabe
Verarbeitungsweise?
Weitergabe?
Umgang mit Ausgabe?

Texte + Bilder

Autonome Mobilität

Strukturen erkennen

Neue Thesen zu KI

- „KI schnackt dumm Tüch“
  - Wie vertrauenswürdig sind die Ergebnisse?
    - Wahrscheinlichkeit von „Halluzinationen“ / Fehlern
    - KI-Selbsteinschätzung der Fehlerwahrscheinlichkeit?

Foto von Bewahrerderwerte – Eigenes Werk, CC BY-SA 4.0

Neue Thesen zu KI

- „KI schnackt dumm Tüch“
  - Gibt es Quellenangaben?
    - Welche Informationen wurden einbezogen?
    - Wie naheliegend sind die hergestellten Bezüge?

Foto von Bewahrerderwerte – Eigenes Werk, CC BY-SA 4.0

Neue Thesen zu KI

- „KI schnackt dumm Tüch“
  - Haben die Ergebnisse einen Bias / Diskriminierung?
    - Erlernte oder neue Diskriminierung
    - Sprachliche Verzerrung

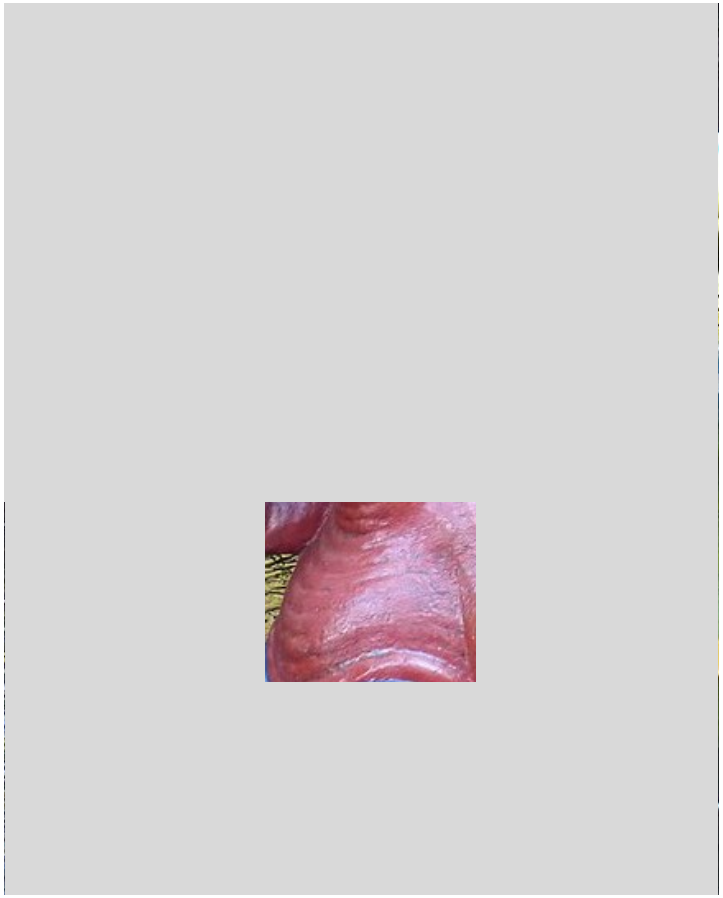

Foto von Bewahrerderwerte – Eigenes Werk, CC BY-SA 4.0

Neue Thesen zu KI

Qualität
Vertrauenswürdigkeit?
Quellenangaben?
Bias/Diskriminierung?

Texte + Bilder

Autonome Mobilität

Strukturen erkennen

Neue Thesen zu KI

- „KI ist wie eine Wurstfabrik“
  - Mit welchen Daten wurde KI trainiert?
    - Personenbezug?
    - Erlaubnis für Nutzung?
    - Sprachliche / kulturelle Verteilung der Trainingsdaten

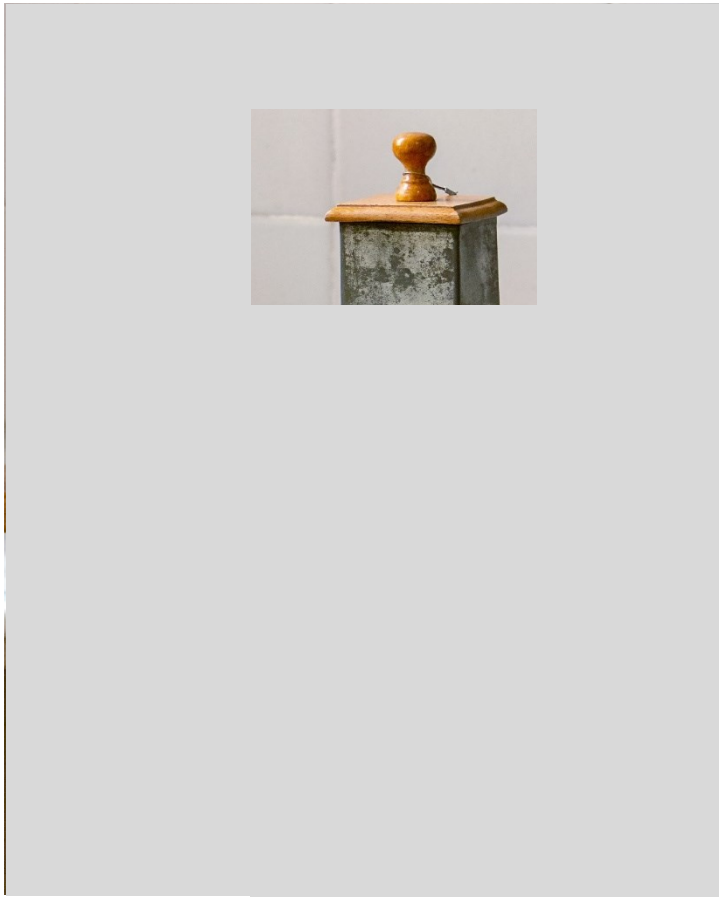

Foto von Maria Krasnova auf Unsplash

Neue Thesen zu KI

- „KI ist wie eine Wurstfabrik“
  - Was wissen wir über das KI-System und die Funktionsweise?
    - Bedeutung / Gewichtung von Eingabedaten
    - Manipulationsmöglichkeiten (Prompt Engineering)
    - Eingebaute Filter und Schranken

Foto von Maria Krasnova auf Unsplash

Neue Thesen zu KI

- „KI ist wie eine Wurstfabrik“
  - Wer sind die Betreiber*innen des KI-Systems?
    - Ideelle oder materielle Interessen / Ziele?
    - Politische und finanzielle Unabhängigkeit?

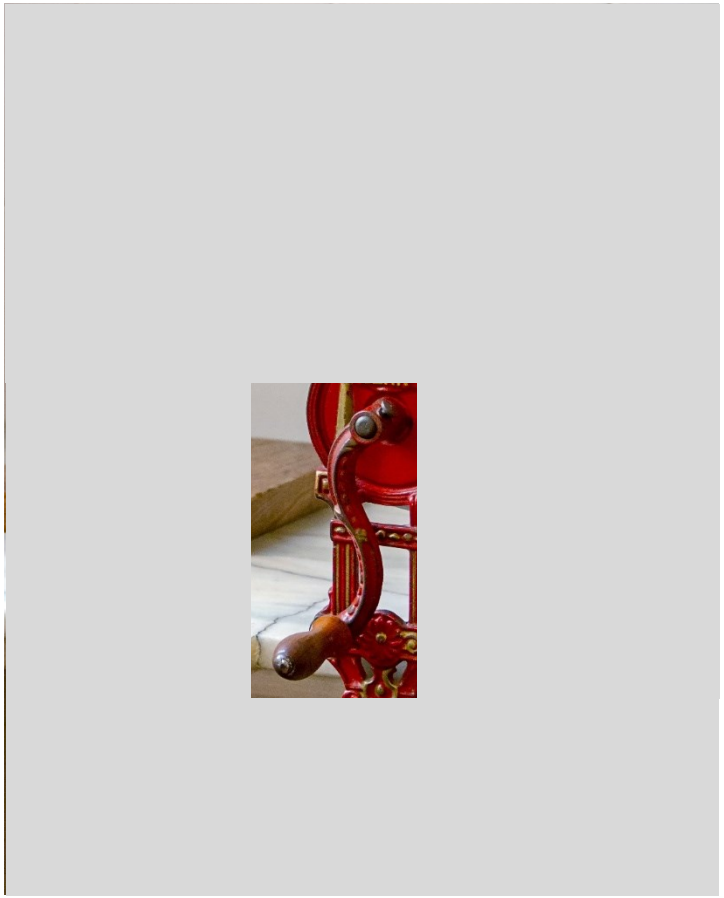

Foto von Maria Krasnova auf Unsplash

Neue Thesen zu KI

Transparenz
Training?
Funktionsweise?
Betreiber*innen?

Texte + Bilder

Autonome Mobilität

Strukturen erkennen

Neue Thesen zu KI

- „KI braucht Aufsichtspersonen“
  - Wie setzt man Betroffenenrechte durch?
    - Auskunftsrechte
    - Recht auf Löschen und Recht auf Korrektur

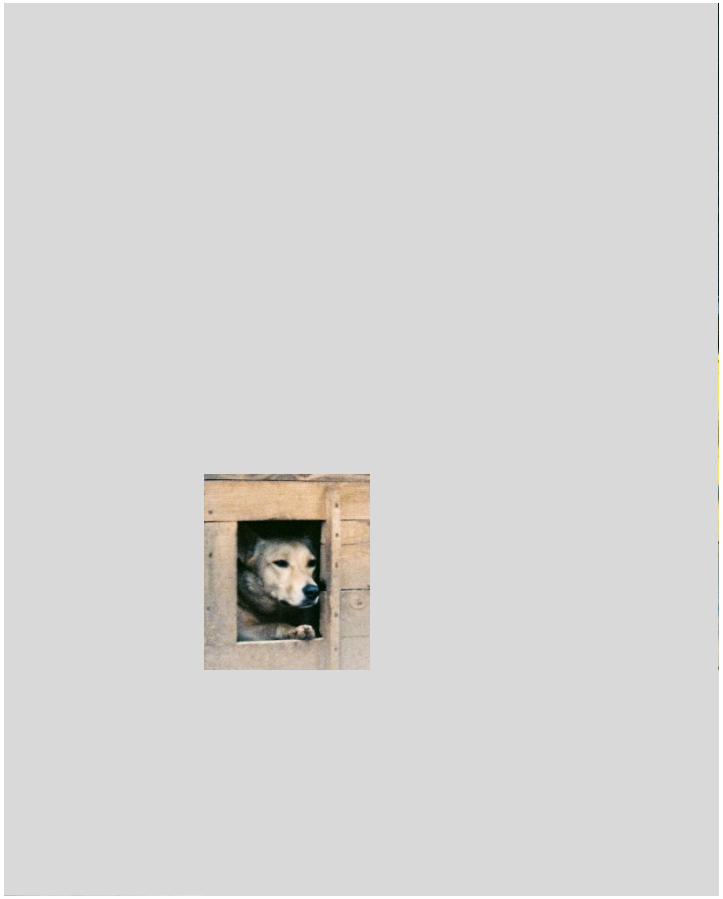

Foto von Jana Shnipelson auf Unsplash

Neue Thesen zu KI

- „KI braucht Aufsichtspersonen“
  - Wer ist verantwortlich?
    - Nutzende?
    - Programmierer*innen?
    - Verantwortliche des KI-Systems?
    - Das KI-System???

Foto von Jana Shnipelson auf Unsplash

Neue Thesen zu KI

- „KI braucht Aufsichtspersonen“
  - Wie sicher ist das KI-System?
    - Datenschutzrechtliche Risikobewertung
      → i.d.R. Datenschutz-Folgeabschätzung nötig
    - IT-Sicherheit des KI-Systems
    - Manipulierbarkeit

Foto von Jana Shnipelson auf Unsplash

Neue Thesen zu KI

Datenschutz
Betroffenenrechte?
Verantwortlichkeit?
Sicherheit?

Texte + Bilder

Autonome Mobilität

Strukturen erkennen

Fazit, Ausblick und Diskussion

Eingabe / Ausgabe
Verarbeitungsweise?
Weitergabe?
Umgang mit Ausgabe?

Qualität
Vertrauenswürdigkeit?
Quellenangaben?
Bias/Diskriminierung?

Transparenz
Training?
Funktionsweise?
Betreiber*innen?

Datenschutz
Betroffenenrechte?
Verantwortlichkeit?
Sicherheit?

Fazit, Ausblick und Diskussion

- Gesellschaftliche Diskussion und ein gemeinsames Verständnis der Rolle von KI und Kenntnis von ihren Risiken ist wichtig.
- Datenschutzrechtlich stellen sich zum Teil neue Fragen.
- Aufsichtsbehörden verfolgen Entwicklung und arbeiten an aktuellen Positionierungen.

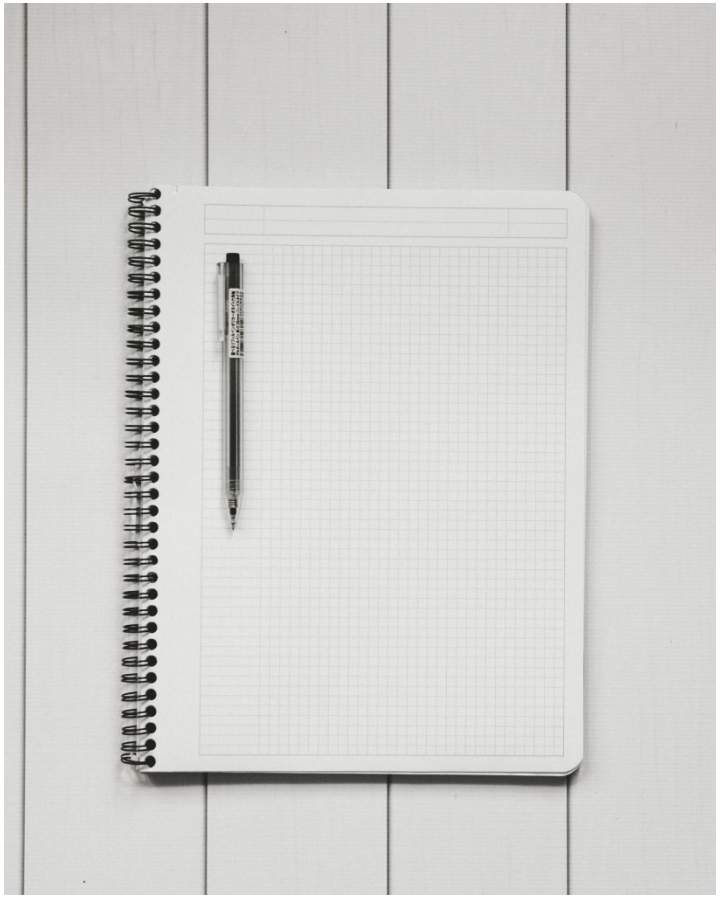

Foto von Kelly Sikkema auf Unsplash

Zum Nachlesen

- **Orientierungshilfe der DSK zu Künstlicher Intelligenz und Datenschutz**
  5. Mai 2024
  https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

- **Empfohlene technische und organisatorische Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen**
  6. November 2019
  Positionspapier der Datenschutzkonferenz
  https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

- **Hambacher Erklärung zur Künstlichen Intelligenz**
  Sieben datenschutzrechtliche Anforderungen
  3. April 2019
  Entschließung der Datenschutzkonferenz
  https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf die Diskussion!