Deutsche Gesellschaft für Recht
und Informatik e.V.

kontakt@dgri.de
www.dgri.de

Geschäftsstelle:
Deutsche Gesellschaft für Recht
und Informatik e.V.
c/o Romy Fiolka, Ass. iur.
Konrad-Zuse-Straße 41
60438 Frankfurt am Main

Sparkasse Karlsruhe
IBAN: DE 27 6605 0101 0022 4047 43
BIC: KARSDE66

**An alle DGRI-Mitglieder und Interessierte**

26. April 2024

**Einladung zur Veranstaltung „AI for Lunch“ des Fachausschusses KI, IoT, Blockchain**

Liebe DGRI-Mitglieder,
liebe Interessierte,

wir laden Sie herzlich ein zum vierten Teil unserer Veranstaltungsreihe „AI for Lunch“ (**#ai4lunch**) mit **Anna Wilhelm**, Referentin im Referat TK 24 – Sicherheit in der Künstlichen Intelligenz – am **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, zu dem Thema:

# KI und IT-Sicherheit

Die Veranstaltung findet online statt via Microsoft Teams am

**Donnerstag, den 29. Mai 2024, von 12:00 bis 13.00 Uhr**.

Den Zugangs-Link zur Teilnahme erhalten Sie nach Anmeldung. Bitte melden Sie sich **bis zum 28. Mai 2024** per E-Mail an **kontakt@dgri.de** an.

## Zum Thema:

Die Veranstaltung ist der vierte Teil der Veranstaltungsreihe „AI for Lunch“ (**#ai4lunch**) rund um das Thema Recht und KI. Ziel der Reihe ist es, die Teilnehmer in die Lage zu versetzen, die Europäische KI-Verordnung mitsamt ihrer tragenden Erwägungsgründe und ihrer Auswirkungen zu verstehen und diskutieren zu können.

Die Reihe setzt sich nach derzeitiger Planung aus den folgenden Terminen zusammen:

1. Technische Einführung
2. Einführung in die Europäische KI-Verordnung
3. KI und ihre Hersteller
4. **KI und IT-Sicherheit**

Im vierten Termin werden wir **KI aus Sicht der Informationssicherheit** diskutieren. Themenschwerpunkte werden neben der Darstellung der Aufgaben des BSI in diesem Kontext u.a. sein:

- IT-Sicherheit für KI,
- IT-Sicherheit durch KI,
- Angriffe auf KI, insbesondere in Form von Poisoning, Evasion und Privacy Attacks.

Diese Aspekte werden dabei exemplarisch am Beispiel großer KI-Sprachmodelle (engl. Large Language Models – LLMs) beleuchtet.

## Zur Referentin:

Anna Wilhelm, im Jahr 1995 geboren in Saarlouis, Studium der Informatik an der Universität des Saarlandes (M.Sc., 2018), war nach ihrem Abschluss vier Jahre lang im IT-Sicherheitsmanagement, zunächst der bayerischen und später der saarländischen Justiz, tätig. Seit Februar 2023 ist sie im Bundesamt für Sicherheit in der Informationstechnik (BSI) am Standort Saarbrücken im Referat TK 24, Sicherheit in der Künstlichen Intelligenz, beschäftigt. Schwerpunkte ihrer Tätigkeit sind dabei IT-Sicherheitsaspekte rund um die Themen Natural Language Processing und Generative Künstliche Intelligenz.

Wir freuen uns auf Ihre Teilnahme!

DGRI-Fachausschuss KI, IoT, Blockchain

**Dr. Viktoria Schmittmann, LL.M. M.Sc.** **Dr. Andreas Sesing-Wagenpfeil**

**Paul F. Welter**