HISCOX

CYBER-BOOTCAMP AM 23. OKTOBER | 09:30 BIS 10:15 UHR

Darf ich das mit KI?
Die wichtigsten Datenschutz-Checks



DR. MARTIN SCHIRMACHER
HÄRTING Rechtsanwälte

Drei Level Datenschutz in der Praxis

3 **Drittstaatentransfer**
Dürfen die Daten in die USA?

Art. 44 ff. DSGVO
Data Privacy Framework
Standardvertragsklauseln

2 **Dienstleister**
Verarbeitet der Anbieter nur für mich – oder auch für sich?

Art. 28 DSGVO
Auftragsverarbeitungsvertrag
keine Eigennutzung (z. B. Training)

1 **Rechtsgrundlage**
Darf ich diese Daten für diesen Zweck überhaupt verarbeiten?

Art. 6 DSGVO
berechtigtes Interesse
Vertrag
Einwilligung

Der KI-Meeting-Assistent

Ein Unternehmen führt einen KI-Assistenten für alle internen Besprechungen und Kundentermine ein.

Einsatz

Transkription

Nimmt an Teams- und Zoom-Calls teil, schreibt mit, fasst zusammen und erstellt To-dos

Dienstleister

SaaS-Anbieter

Standard-AVV des Anbieters ist abgeschlossen
Kein eigenes Training

Sitz des Anbieters

USA

Anbieter ist nach dem EU-U.S. Data Privacy Framework zertifiziert

Zweck

Auswertung

Bewertet Redeanteile, Stimmung und Gesprächsführung jedes Vertriebsmitarbeiters

Ist der Einsatz datenschutzkonform?

Dr. Martin Schirmbacher | Fachanwalt für IT-Recht

HÄRTING

Grundlagen: Personenbezug von Daten

Fast alle Daten haben Personenbezug

Personenbezug
Eindeutig

- Namen und Stimmen im Meeting
- Absender der Eingangspost
- Beschäftigtendaten
- Ansprechpartner in der B2B-Kundenliste

Personenbezug
Über Umwege

- Kundennummer im Werbescoring
- IP-Adresse
- Online-Kennung in Cookies

Personenbezug
Fehlt

- Daten juristischer Personen, z. B. Umsatz der GmbH
- **Aber: Einzelkaufleute und Ein-Personen-GmbH**
- Echt anonymisierte Daten

Pseudonymisiert ist nicht anonym

jedenfalls nicht für Sie, wenn Sie die Zuordnung kennen

Grundlagen: Verbotsprinzip

Verarbeitung personenbezogener Daten ist verboten...
...es sei denn...

- **Einwilligung des Betroffenen**
- und/oder
- **Vertrag oder ähnliche Verbindung**
- und/oder
- **Rechtliche Verpflichtung**
- und/oder
- **Berechtigtes Interesse des Unternehmens**

Verarbeitung personenbezogener Daten ist verboten...
...es sei denn...

- Einwilligung des Betroffenen
- Vertrag oder ähnliche Verbindung
- Rechtliche Verpflichtung
- **Berechtigtes Interesse des Unternehmens**

Prüfungspunkte: Berechtigtes Interesse

1.	**Berechtigtes Interesse**	• **jedes legale auch wirtschaftliche Interesse** • **geeignetes Interesse richtet sich nach dem Verarbeitungszweck**
2.	**Notwendigkeit**	• **bloße Zweckmäßigkeit nicht ausreichend** • **aber auch nicht Erforderlichkeit im engeren Sinne**

3.	**Kein Überwiegen der Interessen der Betroffenen**	• **Gesetzlich anerkanntes Interesse**
		  • Direktwerbung, Betrugsverhinderung
		• **Gesetzlich vermutetes Interesse**
		  • Kundenbeziehung, interne Verwaltungszwecke
		• **Maßgeblich: „vernünftigen Erwartungen der betroffenen Person“**
		• **Erwartungen nicht ohne Weiteres durch Information formbar**

Level 1: Verarbeitung personenbezogener Daten mit KI

Eingangspost: KI sortiert die Briefe

- KI liest eingehende Briefe und E-Mails, erkennt das Anliegen und leitet weiter
- SaaS-Lösung, Anbieter und Rechenzentrum in der EU
- Training nur im Auftrag des Kunden und nur für dessen Instanz

Ergebnis
Berechtigtes Interesse trägt

Level 3 · Drittstaat
entfällt: kein Drittlandsbezug

Level 2 · Dienstleister
AVV, Training nur für den Kunden

Level 1 · Rechtsgrundlage
Berechtigtes Interesse trägt

KI-gestütztes Werbescoring

- Lokales KI-Modell bewertet Kundendaten und steuert, wer welche Werbung erhält
- Betrieb On-Premise, keine Dienstleister, keine Übermittlung
- Datengrundlage: Kaufhistorie, Interaktionen, Profilmerkmale

Ergebnis

Abwägung entscheidet, im Zweifel Einwilligung einholen

Level 3 · Drittstaat
entfällt: kein Transfer

Level 2 · Dienstleister
entfällt: lokaler Betrieb

Level 1 · Rechtsgrundlage
Abwägung Usecase-abhängig, ggf. Einwilligung

Der KI-Meeting-Assistent

- Gleiches Tool, gleicher Vertrag, gleicher Server
- Mitschreiben und Zusammenfassen: erwartbar, berechtigtes Interesse
- Bewertung der Vertriebsmitarbeiter: Leistungskontrolle, Einwilligung im Arbeitsverhältnis kaum freiwillig

Ergebnis
Der Zweck entscheidet



Level 2:
Verarbeitung durch Dritte

Die Kundenliste in ChatGPT

- Vertrieb lädt die Kundenliste hoch und lässt Upselling-Potenziale auswerten
- Vertragspartner ist OpenAI Ireland, verarbeitet wird in den USA
- Entscheidend ist die Lizenz: Free, Plus und Pro ohne AVV, Business und Enterprise mit DPA

Ergebnis

Die Lizenz löst Level 2 und 3, aber nicht Level 1



Level 3:
Verarbeitung außerhalb der EU

Wann liegt ein Drittlandstransfer vor?

	Server in der EU	Server in den USA
Vertragspartner in der EU	**Zunächst kein Transfer** z. B. irische Gesellschaft, Server Amsterdam **Aber: Support und Subprozessoren prüfen**	**Transfer durch den Anbieter** z. B. ChatGPT: OpenAI Ireland, Verarbeitung in den USA **DPF oder SCC erforderlich**
Vertragspartner in den USA	**Transfer** Empfänger sitzt im Drittland, Serverstandort EU **DPF oder SCC erforderlich**	**Transfer** z. B. Meeting-Assistent eines US-Anbieters **DPF oder SCC erforderlich**

Hintertür: Zugriff aus den USA durch Support oder Subprozessoren ist ein Transfer, auch bei EU-Gesellschaft und EU-Server.

Kein Transfer: Die US-Konzernmutter allein. Das Zugriffsrisiko (CLOUD Act) gehört zu Level 2, nicht zu Level 3.

4. HÄRTING KI-Tag

- Praxisnahe Sessions zu KI in der Rechtspraxis
- Expert:innen aus Aufsicht, Regulierung und Unternehmen
- Networking & Austausch in Berlin
- Termin: 19.11.2026

PROGRAMM & TICKETS →

Zusammen-fassung

AI Officer Ausbildung

- Berufsbegleitende Weiterbildung mit Praxisbezug
- Für Unternehmen, Compliance und Datenschutz
- Präsenz- und Online-Termine
- Zertifikat & direkt anwendbares Know-how

INFOS & ANMELDUNG →

Checkliste Datenschutz und KI

Level 1
Rechtsgrundlage

- ☐ Rechtsgrundlage für den Zweck (Art. 6 DSGVO)
- ☐ Löschfristen nach Zweck festlegen
- ☐ Datenschutzinformation um KI-Tools ergänzen
- ☐ Prozesse für Auskunftsanfragen
- ☐ Verarbeitungsverzeichnis anpassen

Level 2
Dienstleister

- ☐ AVV abschließen (Art. 28 DSGVO)
- ☐ Weisungsgebundenheit sicherstellen
- ☐ Keine Nutzung zu eigenen Zwecken, z. B. Training

Level 3
Drittlandstransfer

- ☐ DPF-Zertifizierung prüfen oder SCC vereinbaren
- ☐ ggf. Transfer Impact Assessment (TIA)

Über alle Level: Mitarbeitende schulen: KI-Kompetenz (Art. 4 KI-VO) und klare Regeln für Daten in KI-Tools

HÄRTING

TAG 01

BLOCK 01
Vom Hype zur Realität
KI im Überblick

BLOCK 02
Von der Theorie zur Anwendung
GenAI als Sparringspartner

BLOCK 03
Rechtliche Rahmenbedingungen
KI-Recht in der Praxis: Urheberrecht, Vertragsrecht, Haftung & Co.

BLOCK 04
Datenschutz & KI
Die Grundlagen beim Einsatz von KI

AFTER WORK
Networking
Bei Drinks & Snacks

TAG 02

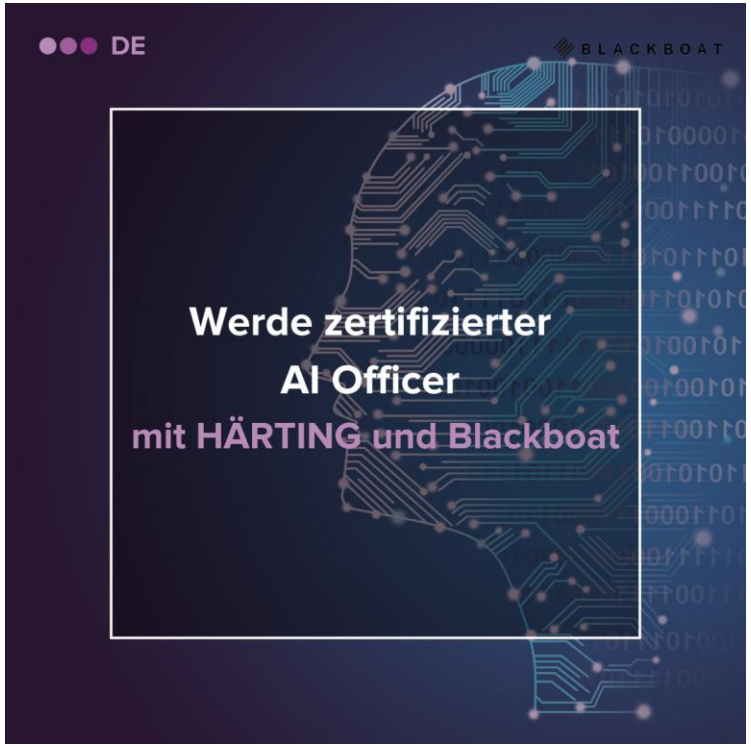
BLOCK 01
Der EU AI Act
Einordnung, Vorgaben und Pflichten

BLOCK 02
AI Compliance & Governance
KI im Unternehmen rechtskonform integrieren und steuern

BLOCK 03
AI-Integration Map – Framework
Zur erfolgreichen Integration von GenAI in Unternehmen

BLOCK 04
Veränderung begleiten
GenAI effektiv im Arbeitsalltag anwenden

FOLLOW-UP
2 digitale Deepdives
Datenschutz &-sicherheit // AIM, Advanced Prompting, Use Cases

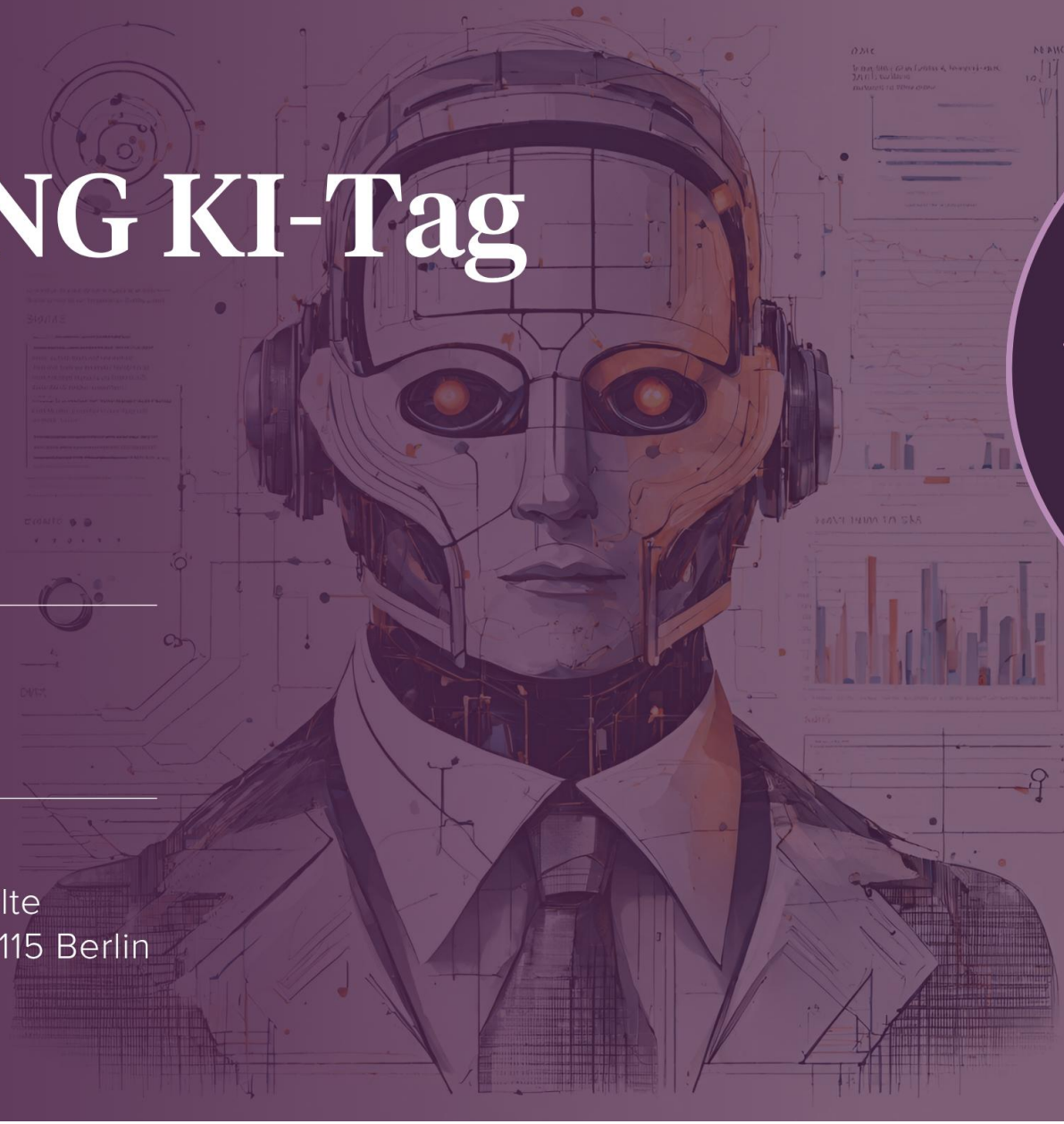


www.ai-officer.io

DE

4. HÄRTING KI-Tag

KI in der (Rechts-)Praxis



Datum
19. November 2026

Uhrzeit
09:30 bis 18:00 Uhr

Ort
HÄRTING Rechtsanwälte
Chausseestraße 13, 10115 Berlin

LETZTE TICKETS

bis zum 12.11.2026
200 € zzgl. MwSt.

*Buchung über Eventbrite

https://haerting.de/wissen/4-haerting-ki-tag-ki-in-der-rechtspraxis/



HÄRTING

Dr. Martin Schirmbacher

Fachanwalt für IT Recht

schirmbacher@haerting.de

Online-Marketing-Recht Seminare:
http://bit.ly/OM-Recht-Seminar

Newsletter zum Datenrecht:
https://data-navigator.eu/newsletter/

HÄRTING Rechtsanwälte | www.haerting.de

Chausseestr. 13, 10115 Berlin | Tel. +49 30 28 30 57 40 | Fax. +49 30 28 30 57 44