



LINET Services GmbH

Ihr regionaler Partner für IT und Compliance in
Braunschweig!



Referenten Anna Bauer & Benjamin Nowosadek

Juristen, Fachkraft für Datenschutz, Compliance
Officer

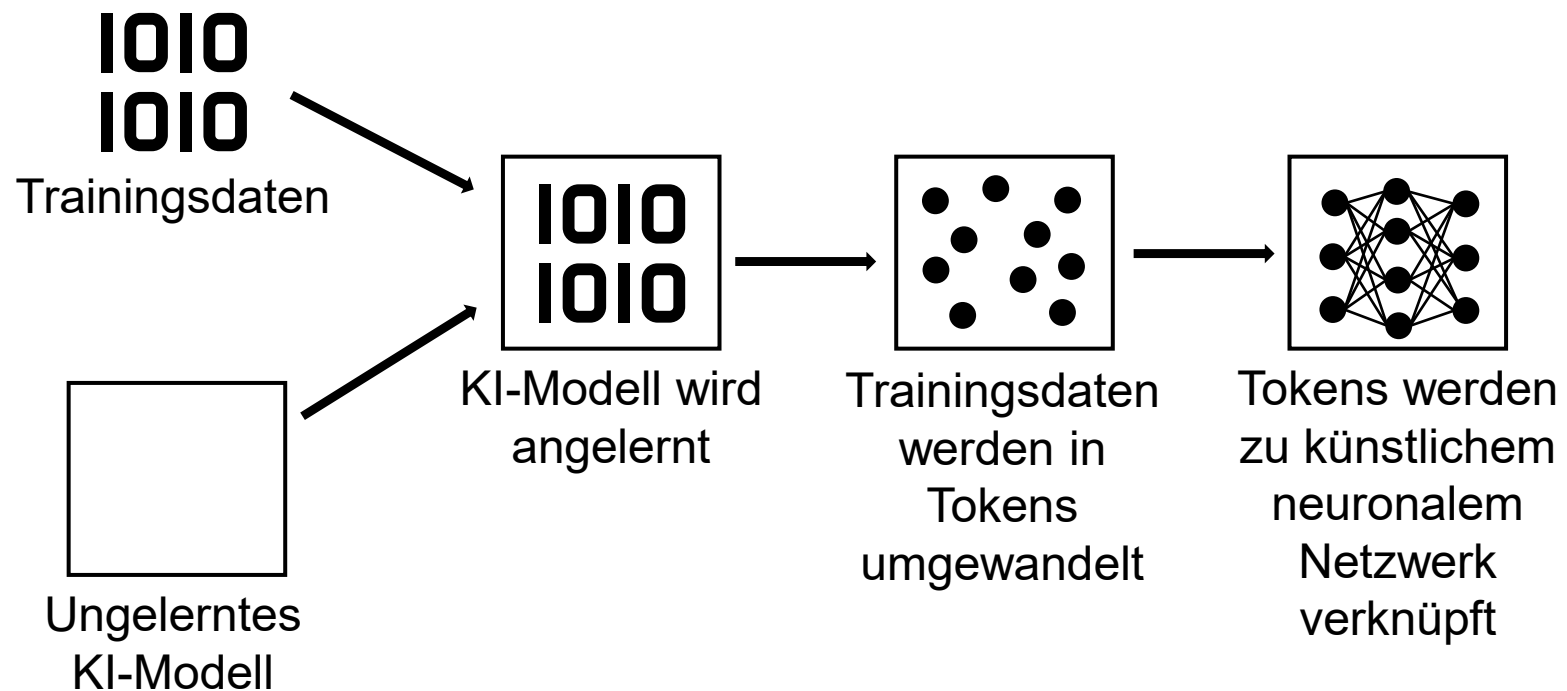


Die Herausforderungen des Datenschutzes im Zeitalter der Künstlichen Intelligenz:

Risiken, Chancen und gesetzliche
Rahmenbedingungen



Die Entstehung von KI



Datenschutz und KI

- Beim Datenschutz geht es ausschließlich um **personenbezogene Daten** und bspw. nicht um Geschäftsgeheimnisse
- KI-Systeme verarbeiten personenbezogene Daten, wenn diese als **Trainingsdaten** oder als **Prompt** eingegeben werden
- Anders als normale Software verarbeitet KI auf **nicht nachvollziehbare Weise** und im großen Umfang zu verschiedenen Zwecken
- Dadurch kann ein Konflikt zwischen Zweckbindung und **adaptiver Datenverwendung** durch die KI entstehen

**Auf die Einhaltung des Datenschutzes muss bei KI daher ein
genaues Augenmerk gelegt werden!**



Risiken für den Datenschutz

„Black Box“- Problem und Transparenz

- Durch die Antwortfindung basierend auf Wahrscheinlichkeiten, ist der genaue Verarbeitungsvorgang der KI nicht ersichtlich, die KI ist eine „Black Box“
- Problem bei der Umsetzung von Betroffenenrechten wie **Löschung, Auskunft, Übertragung** etc.
- Außerdem führt dies zu Problemen bei den **Informationspflichten** ggü. Betroffenen

Beim Einsatz von KI wird es immer Unsicherheiten und Unklarheiten geben!



Risiken für den Datenschutz

Automatisierte Entscheidungen ohne menschliche Kontrolle

- In der DSGVO gibt es das Recht keiner **automatisierten Einzelentscheidung** zu unterliegen
- KI die automatisierte Einzelentscheidungen trifft, könnte als Hochrisiko-KI gelten
- In diesen Fällen sollte sowohl nach DSGVO und nach AI-Act eine **menschliche Aufsicht** in den Prozess integriert werden
- Hochrisiko-KI Systeme ohne menschliche Aufsicht sind nach AI-Act unzulässig; auch nach DSGVO sollte eine menschliche Aufsicht als angemessene Maßnahme ergriffen werden

Eine automatisierte Einzelentscheidung einer KI ohne menschliche Aufsicht sollte unbedingt vermieden werden!



Risiken für den Datenschutz

Abfluss von Informationen an den KI-Anbieter

- Wenn die KI über einen Anbieter als Dienstleistung bezogen wird (bspw. OpenAI, Microsoft), kann der KI-Anbieter alle Eingaben einsehen und ggfls. zum Training der KI verwenden
- Sofern mit dem Anbieter kein Vertrag über das **Auftragsverarbeitungsverhältnis (AVV)** geschlossen wurde, ist diese Weitergabe an Dritte **unzulässig**
- In dem AVV sollte geregelt sein, dass der Anbieter die personenbezogenen Daten nicht zum Training der KI und auch sonst nicht zu eigenen Zwecken verwenden darf

Beim Bezug einer KI über einen Dienstleister sollte daher idR ein AVV abgeschlossen werden!



Chancen durch KI im Datenschutz

Automatisierung von Datenschutzprozessen

- Unterstützung bei der Festlegung und Einhaltung von **Speicherfristen**
- KI unterstütze Prozesse zur **Datenminimierung**
- Automatisierte Klassifikation und Kategorisierung personenbezogener Daten und Zuordnung in das **Verzeichnis der Verarbeitungstätigkeiten**
- Einsatz zur Einhaltung von **Rechenschaftspflichten** durch Dokumentation und Prozessgestaltung



Chancen durch KI im Datenschutz

Erkennung von Datenschutzverletzungen

- KI-gestützte Systeme können bei der **Fehlererkennung** und **Risikobewertung** helfen
- Frühzeitige Identifikation von **Sicherheitsvorfällen**
- Unterstützung bei der **Dokumentation und Meldung** von Verletzungen
- Beitrag zur **Einhaltung und regelmäßiger Kontrolle** technischer und organisatorischer Maßnahmen



Chancen durch KI im Datenschutz

Erfüllung von Betroffenenrechten

- Schnellere und zielgerichtete Bearbeitung von Betroffenenrechten bspw. durch automatisierte Auskunftersuchen
- Abfrage von Betroffenenersuchen durch **KI-Chatbot**, der direkt die Identitätsprüfung durchführt (bspw. durch Abfrage der Kundennummer) und die Anfrage vorbereitet
- KI-Systeme, die in das Firmennetzwerk integriert sind, können personenbezogene Daten schnell heraussuchen und bspw. für ein **Auskunftersuchen oder eine vollumfängliche Löschung vorbereiten**



DSGVO und AI-Act

Einführung in den AI-Act

- Ziel ist die Sicherstellung **vertrauenswürdiger** KI-Systeme in der EU
- Der AI-Act gilt für **Anbieter, Betreiber**, Einführer, Händler etc. von KI-Systemen
- Wenn ein Unternehmen KI **einsetzt**, gilt es als **Betreiber**
- Wenn ein Unternehmen eine KI **entwickelt**, gilt es als **Anbieter**
- AI-Act und DSGVO stehen nebeneinander und ergänzen sich
- Fokus auf Risikomanagement, Transparenz und Schulungen

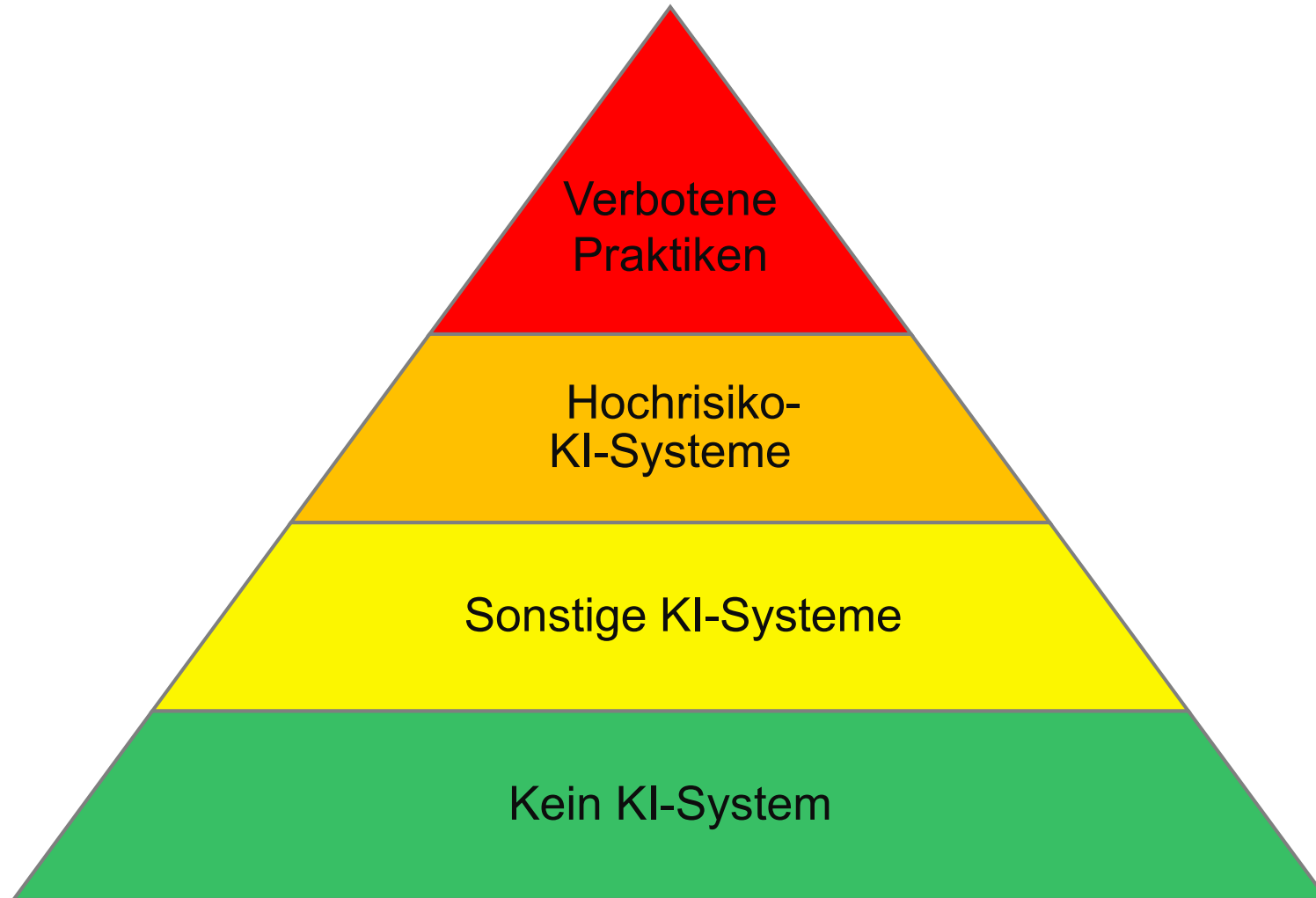


Pflichten aus dem AI-Act

- Sicherstellung der KI-Kompetenz: Schulung der Anwender, damit ein **sachkundiger Einsatz** möglich ist
- Kategorisierung von KI-Systemen
- Bei Hochrisiko KI-Systemen u.a.:
 - Transparenzpflichten
 - Technische und Organisatorische Maßnahmen zur Sicherstellung ordnungsgemäßer Verwendung
 - Sicherstellung menschlicher Aufsicht
 - Überwachung des Systembetriebs
 - Protokoll- und Aufbewahrungspflichten



Kategorisierung von KI-Systemen



Kategorisierung von KI-Systemen

Verbotene Praktiken

- Social Scoring
- Echtzeit-Gesichtserkennung
- Biometrische Kategorisierung
- Emotionserkennung am Arbeitsplatz

Hochrisiko-KI-Systeme

- Credit Scoring (Bonität, Kreditausfallrisiko etc.)
- Verwendung von KI in (digitaler) kritischer Infrastruktur
- Auswahl und Überprüfung im Kontext von Bildungseinrichtungen
- HR-Angelegenheiten (Bewerbersauswahl, Kündigungen, Beförderungen)

Sonstige KI-Systeme

- Chatbots
- Spamfilter
- Suchalgorithmen
- LLMs ausschließlich zur Recherche



Best Practices für Unternehmen

- Der Datenschutz sollte bei der Einführung einer KI **von Anfang an mitgedacht** werden, etwa durch frühzeitige Einbindung des Datenschutzbeauftragten
- Am besten sollte auf die Eingabe von personenbezogenen Daten in KI-Systeme **vollständig verzichtet** werden (Stichwort: richtig prompten!)
- **Interne Richtlinien** sollten den Einsatz von KI regulieren und Mitarbeiter aufklären
- Notwendige **Systeminformationen** sollten - soweit möglich - vom Anbieter des KI-Systems eingeholt werden, um bestmöglich die datenschutzrechtlichen Informationspflichten erfüllen zu können
- Je nach Einsatz, sollte mit dem Anbieter des KI-Systems regelmäßig ein **Auftragsverarbeitungsvertrag** abgeschlossen werden



Best Practices für Unternehmen

- Eine **Einstufung des KI-Systems** nach AI-Act sollte frühzeitig vorgenommen werden
- Insbes. bei Bildgenerierung ist auf **Transparenzpflicht** zu achten
- Für Erreichung der **KI-Kompetenz** der Nutzer sollten entsprechende Ressourcen geschaffen werden
- Ggfls. Einrichtung einer **zentralen Ansprechperson** zum Thema KI
- Die bereits genannte **interne Richtlinien** sollte auch Vorgaben zum AI-Act enthalten (bspw. Festlegung eines Nutzungsrahmens der KI, um ggfls. Hochrisiko-Einsatz zu vermeiden)



Vielen Dank für Ihre
Aufmerksamkeit!

Bei Fragen stehen wir Ihnen
gerne zur Verfügung!

Alle Beiträge des
IT- & Digitalisierungstages
finden Sie online unter
www.it-tag-38.de
zum Download.

