



Ashurst

HISCOX

Checkliste

ChatGPT & Co – was geht und was mach ich besser nicht?

Rechtlicher Hinweis:

Diese Checkliste soll eine erste praktische Orientierung und Hilfestellung bieten, Kontrollfragen beim Einsatz von KI-Systemen zu stellen (insbesondere große Sprachmodelle, den „LLM“, wie z.B. ChatGPT, Perplexity, etc.). Sie dient Schulungszwecken, ist auf keine spezifischen Systeme ausgerichtet und ist unvollständig. Die Liste gibt keinen Überblick zu den einschlägigen Rechtsfragen, wenn ich KI-Systeme nutzen möchte. Sie kann damit auch nicht die qualifizierte Rechtsberatung im Einzelfall ersetzen.

KI – total praktisch, aber woran sollte ich besser vorher denken?

1. Richtiges Prompten

1.1 Was darf ich eingeben?

Nutze ich ein offenes oder gekapseltes (firmen-internes) KI-System?

Wenn ein offenes System: Weiß ich, wo meine Daten verarbeitet werden?

Personenbezogene Daten von Kunden und Mitarbeitern – habe ich die Einwilligung der Betroffenen oder kann ich ein berechtigtes Interesse geltend machen?

Habe ich die Erlaubnis der Autoren, Urheber etc., um Verlagstexte, Filmen, Musikstücke einzugeben und durch die KI bearbeiten zu lassen?

Wichtig: Vorsicht mit personenbezogenen Daten! Bitte außerdem keine Geschäftsgeheimnisse in offene KI-Systeme eingeben!

1.2 Wie gut sind meine Trainingsdaten?

Greift mein Anbieter auf urheberrechtlich geschütztes Material zu und kennzeichnet er mir die Quellen?

Hat mein Anbieter vernünftige Datenschutzhinweise und geht mit personenbezogenen Daten in den Trainingsdaten verantwortungsvoll um?

Gibt es Hinweise des Anbieters und/oder eine firmen-interne Richtlinien zur Nutzung?

Bei gekapselten KI-Systemen: Wer hat meine Trainingsdaten nach Datenschutz, Urheberrecht und mit Blick auf Geschäftsgeheimnisse geprüft und zur Nutzung freigegeben?

1.3 Was ist mit den Ergebnissen?

Weise ich bei redaktionellen und wissenschaftlichen Texten auf den Einsatz von KI-Tools hin?

Habe ich eine menschliche Überprüfung der Ergebnisse eingeplant – auch um Verfälschungen („Bias“) bei wiederkehrender Nutzung von Trainingsdaten zu verhindern?

2. Immer wieder Datenschutz – da war noch was

Weiß ich, wo die KI meine Daten verarbeitet (EU oder in Drittländern?)

Hab ich in meinen Datenschutzhinweisen auf den Einsatz von KI-Tools hingewiesen?

Habe ich mit meinem Datenschutzbeauftragten eine Folgenabschätzung durchgeführt?

Kann ich sicherstellen, dass die betroffenen Personen ihre Rechte mir gegenüber ausüben können, wenn ich ihre Daten mit KI-Tools verarbeite?

3. Was ist mit der KI-Verordnung?

Stelle ich sicher, dass ich keine „verbotenen KI Praktiken“ einsetze und weiß ich, was „Hoch-Risikosysteme“ sind?

Weiß ich, dass KI-Tools zur Prüfung von Kreditwürdigkeit, Bonitätsbewertungen, sowie der Risikobewertung und Preisbildung im Bereich Lebens- und Krankenversicherung als „Hoch-Risikosysteme“ gelten?

Weiß ich, dass ich als Betreiber eines KI-Systems von generativer KI mit allgemeinem Verwendungszweck zum Anbieter eines Hoch-Risikosystems mit allen Pflichten werden kann, wenn ich es so verändere, dass es in den Hoch-Risikobereich fällt?

Habe ich an angemessene Risikomanagementmaßnahmen implementiert, wenn ich Hoch-Risikosysteme in meinem Unternehmen betreibe?

Habe ich die menschliche Überprüfung der Ergebnisse von KI-Tools sichergestellt?

Genüge ich den Schulungspflichten nach Art. 4 KI-Verordnung, wenn ich KI-Systeme in meinem Betrieb systematisch einsetze?
