

# Richtlinie für die Künstliche Intelligenz (KI)

## Versionshistorie

Version	Datum	Anmerkungen	Autor
1.0	03.06.2023	Initialfassung der Leitlinie	Lorenz Macke
2.0	05.07.2023	Korrekturen / Lektorat	
3.0	17.10.2023	Erste 5 Tipps und Gedanken	
4.0	07.05.2024	3.19-23, 5., Tipps und Gedanken ergänzt	
5.0	08.05.2024	Prüffragen und Ausblick ergänzt	
6.0	14.05.2024	§80 auf §90 korrigiert / 4(e) ergänzt ** / Nummerierung / Quiz	

## 1. Einleitung

Bei der MUSTERMANN GMBH kann der Bedarf bestehen, im Internet verfügbare Angebote von Künstlicher Intelligenz (KI) zu nutzen.

Bei der Anwendung von KI ist zu gewährleisten, dass Anforderungen an die Informationssicherheit und datenschutzrechtliche Vorgaben eingehalten werden. Dies soll auch durch die verbindlichen Vorgaben in dieser Richtlinie zum Einsatz von KI umgesetzt werden.

## 2. Geltungsbereich

Diese Richtlinie gilt für alle Standorte der MUSTERMANN GMBH. Sie verpflichtet alle Beschäftigten der MUSTERMANN GMBH zur Einhaltung der hier festgelegten Vorgaben.

## 3. Zulässigkeit des Einsatzes von textbasierten Dialogsystemen unter Nutzung maschinellen Lernens

### 1. Softwarebezeichnung

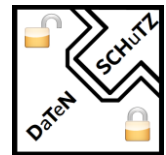
Die Regelung des Einsatzes von ChatGPT des Unternehmens OpenAI.

### 2. Entscheidung

Die finale Entscheidung über den Einsatz des Dienstes trifft

---

in eigener Verantwortung. Für die Beachtung der organisatorischen Vorgaben sowie der weiteren gesetzlichen Bestimmungen bei der Verwendung des Dienstes ist die MUSTERMANN GMBH verantwortlich, die



den Dienst verwendet. Dies gilt auch für die Sicherstellung der sonstigen Rechtmäßigkeit des Einsatzes und die Einhaltung der bei der Verwendung geltenden Nutzungsbedingungen des Anbieters OpenAI.

#### 4. Verwendungseinschränkung

##### 1. Die Verwendung von

- (a) als geheimhaltungsbedürftig eingestuften Informationen (z. B. Geschäftsgeheimnissen),
- (b) sicherheitsrelevanten Informationen,
- (c) Betriebsgeheimnissen sowie
- (d) urheberrechtlich geschützten Informationen, an denen die MUSTERMANN GMBH keine entsprechenden Nutzungsrechte besitzt,
- (e) geschützten Informationen, an denen die MUSTERMANN GMBH Nutzungsrechte besitzt,

zur Erstellung einer Abfrage (Input) ist unzulässig.

[Hinweis: Einstellungsmöglichkeiten der KI, z.B. dass diese die Eingaben NICHT verwendet und NICHT speichert, können nach sorgfältiger vorheriger Prüfung zur Anpassung der Richtlinie 4.1 führen]

##### 2. Die Verwendung von

Informationen, insbesondere personenbezogenen Daten i. S. d. Art. 4 Abs. 1 DSGVO,

oder Informationen, die durch entsprechende Regelungen in den Fachgesetzen nicht veröffentlicht werden dürften,

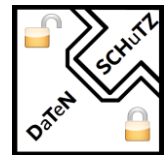
zur Erstellung einer Abfrage (Input) ist unzulässig.

##### 3. Durch die nutzende Person bzw. MUSTERMANN GMBH muss sichergestellt sein, dass die für die Abfrage genutzten Informationen oder Daten frei von Rechten Dritter sind; siehe dazu auch Ziffer 3 (a) Terms of Use (Stand 14.03.2023 – <https://openai.com/policies/terms-of-use>).

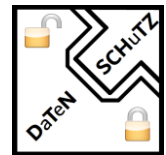
##### 4. Die Nutzung des Dienstes unter Verwendung personenbezogener Daten zum Zweck der Erstellung von Beurteilungen der Persönlichkeit, der Arbeitsleistung, der physischen und psychischen Belastbarkeit, der kognitiven oder emotionalen Fähigkeiten von Menschen, der Erstellung von Prognosen über die Straffälligkeit einzelner Personen oder Personengruppen ist unzulässig.

##### 5. Die unmittelbare Verwendung der durch den Dienst erstellten Textbausteine (Output) zum Zweck des \_\_\_\_\_, \_\_\_\_\_ und \_\_\_\_\_ ist unzulässig.

[Hier kann ein Passus stehen, wofür der Einsatz zulässig ist]



6. Werden die Ergebnisse des Dienstes (Output) ganz oder teilweise zur Erstellung von Texten im \_\_\_\_\_ Kontext, z. B. zur Generierung von Textbeiträgen, Bausteinen für Reden und Antworttexten, Begründung von Entscheidungen oder Vermerken verwendet, ist dies durch die Formulierung: *„Unter Verwendung des textbasierten Assistenzsystems ChatGPT – <https://chat.openai.com/> erstellt.“* kenntlich zu machen.
7. Die Abfrage (Input) ist zusammen mit dem Ergebnis (Output) Teil des ziel findenden Handelns und zusammen mit dem Gesamtvorgang zu den Akten/zur Dokumentation zu nehmen.
8. Der Dienst kann ungenaue Informationen über Personen, Orte oder Fakten erstellen, daher sind Beschäftigte der MUSTERMANN GMBH verpflichtet, die fachliche und sachliche Korrektheit der erstellten Ergebnisse über eine unabhängige Quelle vor der Verwendung zu dienstlichen Zwecken zu überprüfen. Die gilt auch für diskriminierende oder dem deutschen Recht widersprechende Ergebnisse.
9. Die MUSTERMANN GMBH muss in eigener Verantwortung sicherstellen, dass der Schutz der gegenüber OpenAI zur Nutzung des Dienstes ggf. übermittelten personenbezogenen Daten, insbesondere Account Informationen der Beschäftigten, beachtet wird, z. B., indem Funktions-Accounts angelegt werden und für die Nutzung des Dienstes keine privaten Accountdaten verwendet werden.
10. Der Dienst darf ausschließlich dienstlich genutzt werden. Eine private Nutzung ist ausgeschlossen. Die dienstliche Nutzung von privaten Accounts ist ebenfalls ausgeschlossen.
11. Bitte seien Sie sich im Klaren darüber, dass das Ergebnis (Output) keiner Exklusivität unterliegt und somit auch von Dritten erzeugt werden kann. Zudem weisen die Ergebnisse manchmal eine bestimmte Struktur auf, die von Dritten als ChatGPT-Output erkannt wird. Es besteht die Möglichkeit, dass in den Antworttexten von ChatGPT eine Art digitales Wasserzeichen (z. B. charakteristische Abfolge von Buchstaben über mehrere Wörter hinweg) enthalten ist, mit dem nachgewiesen werden kann, dass der Text mittels ChatGPT erstellt wurde. Eine Kennzeichnung der mithilfe von ChatGPT erzeugten Texte schafft Transparenz und verhindert eine „Ent-hüllung“ durch Dritte, dass in der MUSTERMANN GMBH heimlich ChatGPT eingesetzt wird.
12. Arbeitsergebnisse eines KI-Tools dürfen nicht ohne menschliche Überprüfung einer weiteren Verwendung zugeführt werden. Ungeprüfte Arbeitsergebnisse eines KI-Tools müssen als solche gekennzeichnet werden.
13. Die bearbeitende Person entscheidet nach der Generierung des Outputs, ob das erstellte Ergebnis für die zu erledigende Aufgabe eingesetzt und ob das gelieferte Ergebnis angenommen, abgelehnt oder unter Verwendung neuer Parameter wiederholt zur Bearbeitung gestellt wird.



14. ChatGPT kann ein Ergebnis (Output) liefern, das unter Umständen einem bereits urheberrechtlich geschützten Text entspricht.
15. Maßnahmen zur Risikominderung bzw. zum Ausschluss von der Verwendung von eventuell urheberrechtlich geschütztem Material: \_\_\_\_\_
16. Die Verwendung des Dienstes zu illegalen Aktivitäten, Umgehung dieser oder Verbreitung dieser ist unzulässig.
17. Überprüfen Sie, ob der Output gegen mögliche Gesetze verstößt (z.B. Gleichbehandlungsgesetz).
18. Überprüfen Sie, ob der Output mit einem im Unternehmen möglicherweise vorhandenem „Code of Conduct“ vereinbar ist.
19. Die KI bietet möglicherweise eine Historie der Eingaben. Weitere Teilnehmende könnten Ihre Fragen sehen. Ob und wann die Historie zu löschen ist, ist wie folgt geregelt: \_\_\_\_\_
20. Eingaben zur Manipulation der KI sind unzulässig.
21. Bei Systemen wie Chat GPT (bzw. LLM) basiert der Output auf überwiegend Wahrscheinlichkeiten (und nicht unbedingt auf Richtigkeiten). Seien Sie sich dessen bewusst!

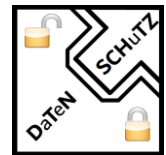
## 5. Missbrauchskontrolle

Bevorzugt findet zuerst eine nicht-personenbezogene Kontrolle der Einhaltung dieser Richtlinie statt, sei es auch nur stichprobenhaft z.B. durch Auswertung von Protokollen. Falls Kontrollen nicht über Protokolle möglich sind, können Stichprobenkontrollen stattfinden.

## 6. Sanktionen

Ein Verstoß gegen diese Richtlinie kann eine arbeitsvertragliche Pflichtverletzung und entsprechend sanktioniert werden.

=====  
*Muster zur kostenfreien internen Verwendung (keine weitere Verbreitung ©).  
Es handelt sich hierbei um VORSCHLÄGE, die anzupassen und betriebsintern zu genehmigen sind. Verwendung auf eigene „Gefahr“.*  
*Inspiration: [transparenz.schleswig-holstein.de/dataset/einsatz-chatgpt](http://transparenz.schleswig-holstein.de/dataset/einsatz-chatgpt)  
(Stand 2.5.2023) gekürzt und ergänzt durch Lorenz Macke ([www.dtnschtz.de](http://www.dtnschtz.de))  
Die Punkte 1+2+6 basieren auf Muster vom [www.Datenschutz-Guru.de](http://www.Datenschutz-Guru.de)  
Weitere Inspiration Mai 2024 durch  
[datenschutz-hamburg.de/news/checkliste-zum-einsatz-llm-basierter-chatbots](http://datenschutz-hamburg.de/news/checkliste-zum-einsatz-llm-basierter-chatbots)  
Die Punkte 4.16 bis 4.23 & 5 sind eigene Hinweise.*



### Zwischendurch etwas Werbung:

(Kostenfreie) Muster zur Sensibilisierung der Mitarbeitenden als PDF  
<http://www.derdsb.de>

Mitarbeitende im Büro/ Home-Office online sensibilisieren?

<https://www.dtnschtz.de/datenschutz-mitarbeiter-sensibilisieren/>

Mitarbeitende zum Datenschutz online schulen?

<https://www.dtnschtz.de/mitarbeiter-schulung-online-zertifikat/>

Vorgehensweise: Passen Sie dieses Muster für sich an oder nutzen Sie es als CHECKLISTE. Eventuell ist das Muster auch für weitere KI-Anwendungen hilfreich.

OB KI eingesetzt wird, regelt das Unternehmen

Falls der Einsatz verboten ist, kann diese Richtlinie entsprechend gekürzt werden oder der Einsatz geht schon aus der Software-Richtlinie hervor.

WIE KI eingesetzt wird, regelt diese Richtlinie.

Ergänzen

Sie gerne den Punkt 4.1, falls Ihnen noch weitere Punkte einfallen, bei denen KI NICHT verwendet werden darf.

Bei 3.15 könnten z.B. Vorgaben zur Recherche und deren Dokumentation stehen.

Bei 3.19 ist die Empfehlung, dass Mitarbeitende selber bestimmen, wann Sie die Historie löschen.

Wie können die Richtlinien verbindlich gemacht werden:

Sie können das Dokument unterzeichnen (zur Kenntnis) lassen.

Als Dokument über das Intranet verbreiten. Anschließend die betreffenden Personen per E-Mail über die Richtlinie informieren. Optional den Erhalt der E-Mail bzw. die Kenntnisnahme der Richtlinie per E-Mail Antwort bestätigen lassen

Das Dokument per E-Mail an die entsprechenden Personen senden. Optional kann man Erhalt der E-Mail bzw. die Kenntnisnahme der Richtlinie per Antwort bestätigen lassen.

Sie haben bereits eine Regelung, wie Richtlinien verbreitet und verbindlich werden.

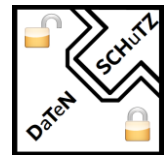
Weitere Tipps und Gedanken zum KI-Einsatz von Lorenz Macke (DtnSchtz):

Die KI wurde mit Daten angereichert, die unter Umständen urheberrechtlich geschützt sind.

Da es meiner Meinung nach ungeklärt bzw. nicht ausgeschlossen ist,

ob ChatGPT bzw. die KI den Output so gestaltet,  
sodass KEINE Rückschlüsse auf original angereicherte Daten besteht,  
besteht ein Restrisiko. Tipp: Output markant abwandeln!

Der Output selber ist (je nach Nutzungsbedingungen) in der Regel nicht geschützt, da der gleiche Output auch von Dritten generiert werden könnte.



Bezüglich des Urheberrechts am Output besteht auch meiner Meinung nach weiterhin allgemeiner Klärungsbedarf (Stand Mai 2024). Je nach „Schöpfungstiefe“ kann ein Urheberrechtsanspruch generiert werden. Zudem ist zu prüfen, ob der Output geschütztem Material „zu sehr ähnelt“ und somit bei Verwendung einem Urheberrechtsverstoß gleichkommt.

Was Sie sonst noch regeln sollten:

An wen können sich Mitarbeitende bei Fragen wenden?

Bei der Beauftragung von Dienstleistern oder der Tätigkeit als Dienstleister ist es ratsam, die Verträge dahingehend zu überprüfen, ob eine Regelung zum Einsatz von KI enthalten ist. Sofern dies nicht der Fall ist, sollte eine entsprechende Regelung ergänzt werden. Beispielsweise kann ein Dienstleister Texte erstellen. Es besteht jedoch auch die Möglichkeit, dass der Dienstleister mithilfe von KI Entscheidungen trifft oder dass ein Produkt mithilfe von KI arbeitet.

Der Arbeitgeber hat den Betriebsrat über die Planung von Arbeitsverfahren und Arbeitsabläufen einschließlich des Einsatzes von Künstlicher Intelligenz rechtzeitig unter Vorlage der erforderlichen Unterlagen zu unterrichten. §80(1) Abs. 3 BetrVG !!!

Vor dem Einsatz von KI sollte gemäß der Meinung der Datenschutzaufsichtsbehörden eine Datenschutzfolgenabschätzung durchgeführt werden. Wenn eine Datenschutzfolgenabschätzung durchzuführen ist, ist ein Datenschutzbeauftragter für das einsetzende Unternehmen zu benennen. Der Datenschutzbeauftragte ist bei der Erstellung der Datenschutzfolgenabschätzung zu Rate zu ziehen!!!

Ob die KI eingesetzt wird, mag möglicherweise auch davon abhängen, WIE die KI trainiert wurde bzw. die Ergebnisse beeinflusst werden. Stichworte sind u.a.: Gleichbehandlung, Vernachlässigung, einseitig, veraltet, unzulässige Erfassung von (personenbezogenen) Daten... mit der Firmenphilosophie vereinbar?

Die vereinfachte Empfehlung bezüglich KI und Datenschutz ist:

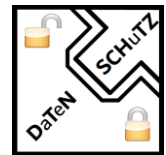
Geben Sie nur personenbezogene Daten ein, wenn Sie diese auch wieder entfernen können bzw. absolut sichergestellt ist, dass das System mit Ihren Daten NICHT trainiert wird. Das wird bei „geschlossenen Systemen“ (Ihr System, Ihre Daten, Ihre Kontrolle) einfacher sein als bei „offenen“ Systemen (Cloud, ChatGPT, unbekannte Anzahl an Nutzern).

Der Einsatz von kostenpflichtigen Versionen bietet die Möglichkeit, Einstellungen datenschutzfreundlicher vorzunehmen.

Prüfen Sie, ob geschlossene Systeme wirklich geschlossen bleiben.

Falls die vorgenannte Prüfung eine Voraussetzung für die Eingabe von personenbezogenen Daten erfüllt, dann ist zu prüfen, ob für die Eingabe der Daten überhaupt eine Rechtsgrundlage vorhanden ist bzw. ob es sich um eine zulässige Zweckänderung handelt.

Bei geschlossenen Systemen können die getätigten Eingaben (die das System trainieren) durch Outputs anderen Mitarbeitenden zugänglich werden.



## Bonus:

### KI & DSGVO

#### Fragen der Aufsicht

#### Prüffragen bei Einsatz von KI-Anwendungen als „Software as a Service (SaaS)“

- Welches Unternehmen betreibt die eingesetzten SaaS? Welches konkrete SaaS-Produkt wird eingesetzt?
- Zu welchen Zwecken wird die SaaS eingesetzt?
- Auf welche Rechtsgrundlage stützen Sie die Verarbeitung personenbezogener Daten zu diesem Zweck?
- Werden die von Ihnen übermittelten Daten vom SaaS-Anbieter zu Trainingszwecken verwendet?
- Liegt eine Auftragsverarbeitung oder gemeinsame Verantwortlichkeit vor? Wenn ja, legen Sie die entsprechende Vereinbarung gemäß Art. 26 oder 28 DSGVO vor.
- Wie werden im Blick auf die o.g. Verarbeitungen die Transparenzpflichten aus Art. 13 f. DSGVO gewahrt?
- Werden die Ausgaben der SaaS als Grundlage für eine Entscheidung mit Wirkung für betroffene Personen genutzt? Werden die Ergebnisse von einem Menschen überprüft? Wenn ja, wie?

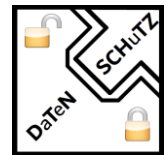
Quelle: Vortrag Herr Thomas Fuchs

Der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit

Vortrag „KI-VO und Datenschutz“

Informationen per Foto von der Präsentation (auf Leinwand) aufgenommen.

Stand 7.5.2024



#### Ausblick:

Welche Einstellungen bei der Software müssen Sie vornehmen (können) und welche Prozesse, Richtlinien, Schulungen, Verträge, technische und organisatorische Maßnahmen müssen im Unternehmen vorhanden sein, damit Software „DSGVO konform“ eingesetzt werden kann? Beobachten Sie die Entwicklung und Empfehlungen!

#### Motivation:

Mindern Sie Ihr Risiko! Je mehr Sie im Unternehmen regeln, desto geringer ist das Risiko für das Unternehmen. Im Zweifel könnte statt des Unternehmens die Person haften, die gegen diese Richtlinie verstößt.

Für Rückfragen und Beratung zum Einsatz von KI stehe ich gerne zur Verfügung.  
Danke für den Download.

Über eine Google Bewertung oder eine freundliche Rückmeldung freue ich mich unter [www.DtnSchtz.de/Danke](http://www.DtnSchtz.de/Danke)

Ich lerne von Ihren Hinweisen und Fragen, damit die nächste Version für alle noch besser wird: 0511 55 19 11 (Telefon Lorenz Macke) oder per E-Mail/ Formular.

Mit datenschutzfreundlichen Grüßen  
Lorenz Macke / Hannover [www.dtnschtz.de](http://www.dtnschtz.de)

#### **Wenden Sie Ihr neues Wissen an!**

10 Quiz Fragen an Mitarbeitende, die KI-Schulung basierend auf dieser Richtlinie. Dauer 1 bis 10 Minuten, kostenfrei und anonym. Schaffen Sie die 100%?  
<https://www.dtnschtz.de/ki-schulung-mitarbeiter-kostenfrei-quiz/>

10 Quiz Fragen an Entscheider/ Verantwortliche, die KI-Schulung basierend auf dieser Richtlinie. Dauer 1 bis 10 Minuten, kostenfrei und anonym. Schaffen Sie die 100%?  
<https://www.dtnschtz.de/ki-schulung-kostenfrei-quiz-verantwortliche/>