RMPRIVACY

13. August 2024

Checkliste zur Einführung einer KI-Anwendung ins Unternehmen

[Firma]

RMPRIVACY GmbH
Große Langgasse 1A
55116 Mainz

A. Checkliste zur Einführung einer KI-Anwendung ins Unternehmen

Die nachfolgende Checkliste soll eine Hilfestellung für die Einführung von KI-Anwendungen im Unternehmen sein, um einen Überblick über die rechtlichen Voraussetzungen zu erhalten und welche gesetzlichen Vorgaben erfüllt werden müssen. Neben der neuen KI-Verordnung (KI-VO) der EU, die seit dem 02. August in Kraft ist, müssen meistens auch die Vorgaben der Datenschutz-Grundverordnung (DSGVO) beachtet werden.

1 Räumlicher Anwendungsbereich

Soll die Anwendung für Nutzer in der EU zur Verfügung stehen?

☐ Ja ☐ Nein

Richtet sich der Output der KI an EU-Bürger?

☐ Ja ☐ Nein

Wenn ja, dann muss die [Firma] die Vorgaben der KI-Verordnung der EU beachten.

2 Anbieter oder Nutzer?

2.1 Soll ein KI-System entwickelt werden, um es unter dem **eigenen Namen** oder der **eigenen Marke** in den Verkehr gebracht oder in Betrieb genommen werden?

☐ Ja ☐ Nein

Wenn ja, dann wird die [Firma] zum Anbieter/Provider im Sinne des Art. 3 Nr. 2 KI-VO.

2.2 Soll ein KI-System **in eigener Verantwortung** im Rahmen einer beruflichen Tätigkeit **verwendet** werden?

☐ Ja ☐ Nein

Wenn ja, dann wird die [Firma] zum Nutzer/Deployer im Sinne des Art. 3 Nr. 4 KI-VO.

3 Welche KI-Anwendung soll genutzt werden?

☐ Microsoft Copilot

☐ Atlassian AI

☐ Large Language Model (LLM), wie ChatGPT, Grog, Perplexity etc.

☐ Chatbot

[Kommentar]

4 Wie soll die geplante KI-Anwendung genutzt werden?

4.1 Werden personenbezogene Daten mit dem KI-System verarbeitet?

☐ Ja ☐ Nein

4.2 Welche Anwendungen sollen KI nutzen?

☐ keine bestimmte Anwendung soll KI nutzen

☐ JIRA Software

☐ JIRA Service Management

☐ JIRA Work Management

☐ Confluence

☐ Trello

☐ Bitbucket Cloud

☐ M365

☐ Microsoft Copilot (ehem. Bing Chat Enterprise)

☐ Windows Copilot

☐ Azure AI Studio

☐ andere: Klicken oder tippen Sie hier, um Text einzugeben.

4.3 In welchem Zusammenhang soll die KI genutzt werden?

☐ Soll durch das KI-System eine unterschwellige Beeinflussung von Personen realisiert werden, um ihnen Schaden zuzufügen?

☐ Soll die Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen genutzt werden, um ihnen Schaden zuzufügen?

☐ Soll die Vertrauenswürdigkeit von Personen aufgrund ihres sozialen Verhaltens oder ihrer Persönlichkeitsmerkmale bewertet oder klassifiziert werden?

☐ Soll ein biometrisches Fernidentifizierungssystem in Echtzeit und in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken verwendet werden?

! **Hinweis RMP**: Falls einer dieser oben genannten Punkte zutrifft, liegt ein **verbotenes System nach Art. 5 KI-VO** vor und der Einsatz des geplanten KI-Systems kann voraussichtlich nicht stattfinden.

Weitere Nutzungsmöglichkeiten:

☐ Biometrisches Echtzeit-Fernidentifizierungssystem oder Möglichkeit der nachträglichen biometrischen Fernidentifizierung

☐ Verwendung als Sicherheitskomponente in der Verwaltung und im Betrieb des Straßenverkehrs sowie in der Wasser-, Gas-, Wärme- und Stromversorgung

☐ Entscheidung über den Zugang oder Zuweisung zu Einrichtungen der allgemeinen und beruflichen Bildung

☐ Bewertung von Schülern in Einrichtungen der allgemeinen und beruflichen Bildung

☐ Bewertung der Teilnehmer an für die Zulassung zu Bildungseinrichtungen erforderlichen Tests

☐ Sichtung, Auswahl und Bewertung von Bewerbungen

☐ Entscheidung über Beförderungen und Kündigungen von Personal

☐ Überwachung und Bewertung der Leistung und des Verhaltens von Personal

☐ Beurteilung von Ansprüchen auf Unterstützungsleistungen

☐ Prüfung und Bewertung von Kreditwürdigkeiten

! **Hinweis RMP:** Falls einer der oben genannten Punkte zutrifft, liegt höchstwahrscheinlich ein **Hochrisiko-KI-System** nach Artt. 6 ff. KI-VO vor und es müssen weitere Voraussetzungen beachtet werden (s. **Ziffer 5**).

☐ Emotionserkennungssystem

☐ Interaktion mit natürlichen Personen, z.B. Chatbot auf der Webseite

☐ Erzeugung oder Manipulation von Bild-, Ton, oder Videoinhalten oder ähnlichem

☐ andere: [Kommentar]

! **Hinweis RMP**: Trifft einer der obig genannten Punkte zu, müssen die Transparenzpflichten nach Art. 50 KI-VO beachtet werden.

5 Liegen alle Voraussetzungen für den Einsatz des Hochrisiko-KI-Systems vor?

Diese Ziffer ist nur relevant, wenn wahrscheinlich ein Hochrisiko-KI-System vorliegt.

5.1 Wurde Ziffer 2.1 mit „Ja“ beantwortet, müssen die nachfolgenden Voraussetzungen eingehalten werden.

☐ Qualitätsmanagementsystem, Art. 17 KI-VO

☐ Testverfahren

☐ Entwicklung mit Trainings-, Validierungs- und Testdatensätzen unter Berücksichtigung der Daten-Governance- und Datenverwaltungsverfahren

☐ Sicherstellung der Beobachtung des KI-Systems nach Inverkehrbringen

☐ Sicherstellung der menschlichen Aufsicht

☐ Sicherstellung der Cybersicherheit

☐ Technische Dokumentation nach Art. 11 KI-VO i.V.m. Anhang IV

☐ Sicherstellung des Konformitätsbewertungsverfahrens, Art. 43 KI-VO

☐ Registrierungspflicht erfüllt, Art. 49 KI-VO

☐ CE-Kennzeichnung, Art. 48 KI-VO

☐ Sicherstellung der Zusammenarbeit mit den Aufsichtsbehörden, Art. 21 KI-VO (beispielsweise durch einen konkreten Ansprechpartner für KI im Unternehmen)

☐ bei Unternehmen mit ausschließlichen Niederlassungen außerhalb der EU: Benennung eines Bevollmächtigten in der EU, Art. 22 KI-VO

5.2 Wurde Ziffer 2.1 mit „Ja“ beantwortet, müssen die nachfolgenden Voraussetzungen eingehalten werden.

☐ Sicherstellung der Verwendung und des Einsatzes nach Gebrauchsanweisung

☐ Sicherstellung der Überwachung des Betriebs nach Gebrauchsanweisung

☐ Aufbewahrung der Protokolle

☐ Durchführung einer Datenschutz-Folgenabschätzung nach der DSGVO, Art. 13 KI-VO

☐ Grundrechte-Folgenabschätzung nach Art. 27 KI-VO

6 Wurde eine Schwellwertanalyse hinsichtlich der Erforderlichkeit einer Datenschutz-Folgenabschätzung durchgeführt?

☐ Ja ☐ Nein

7 Erfolgt eine Datenweitergabe an OpenAI?

☐ Ja ☐ Nein

Wenn ja, wie erfolgt die Weitergabe an OpenAI?

☐ Verschlüsselt ☐ Unverschlüsselt

Ist eine AVV/DPA mit OpenAI abgeschlossen worden?

☐ Ja ☐ Nein

8 Erfolgt eine weitergehende Datennutzung für andere Kunden durch den Anbieter des geplanten KI-Systems?

☐ Ja ☐ Nein

9 Kann zu dieser Datennutzung nach Ziffer 7 aktiv zugestimmt oder diese abgelehnt werden?

☐ Ja ☐ Nein

10 Datenübertragung außerhalb der eigenen Site

[Kommentar]

! Hier wäre zu prüfen welche Funktionalitäten final eingesetzt werden und welche weiteren Subdienstleister zum Einsatz kommen.

11 Wo werden die Daten verarbeitet?

[Kommentar]

! Klärung der vereinbarten Datenresidenz und Speicherung von Produktionsdaten in der ausgewählten Region.

! Wo werden die Daten verarbeitet, wenn sie an OpenAI weitergeleitet werden?

12 Können die Daten, die an das geplante KI-System übermittelt werden, eingeschränkt werden?

[Kommentar]

! **Kontrolle der Datenzugriffe**: Es ist in den Konfigurationen festzulegen, welche Sites und Produkte auf Atlassian Intelligence zugreifen können.

13 Berücksichtigung bestehender Berechtigungen

[Kommentar]

! **Berechtigungsmanagement**: Es ist sicherzustellen, dass der Anbieter des KI-Systems vorhandene Berechtigungsstrukturen respektiert und keine Inhalte außerhalb dieser Berechtigungen erstellt.