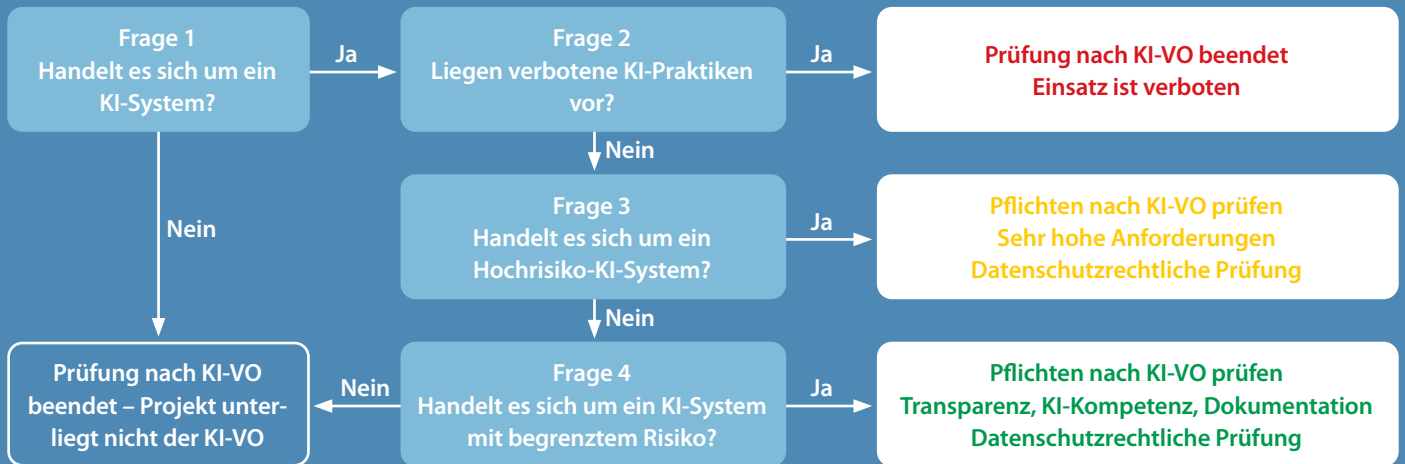




Die empfohlenen Prüfschritte beim Einsatz eines KI-Systems im schematischen Ablauf

Einsatzbeispiel Unternehmens-Podcast

Nutzung echter Stimmen für KI-generierte Inhalte

Ein Unternehmen möchte mithilfe von KI einen Podcast für Kundinnen und Kunden auf der eigenen Website anbieten – und vielleicht künftig weitere Inhalte vertonen. Das Marketing plant, die Stimme eines Mitarbeiters als KI-Stimme zu verwenden. Was ist dabei zu beachten?

Die Veröffentlichung eigener Podcasts ist in Unternehmen immer beliebter, um Kundinnen und Kunden direkt zu erreichen und ihnen Einblicke „hinter die Kulissen“ zu geben. Podcasts zielen oft darauf ab, Nähe aufzubauen und das Unternehmen authentisch wirken zu lassen. Eine KI-generierte Stimme kann hier schnell das Gegenteil bewirken.

Verwendet das KI-System hingegen die Stimme eines echten Mitarbeiters, lässt sich der Produktionsaufwand reduzieren und der gewünschte persönliche Charakter geht so nicht gänzlich verloren. Dabei müssen Unternehmen aber die rechtlichen Anforderungen prüfen und umsetzen. Wie gehen Sie an eine solche Prüfung am besten heran?

Die Grafik oben zeigt die empfohlenen Prüfschritte im Sinne der KI-Verordnung (KI-VO) im schematischen Ablauf. Die nachfolgenden fünf Fragen sind zu beantworten.

1. Handelt es sich um ein KI-System?

Zunächst ist zu prüfen, ob bei dem zuvor beschriebenen Podcast tatsächlich ein KI-System im Sinne der KI-VO die Stimme des Mitarbeiters verarbeitet. Nach Art. 3 Nr. 1 KI-VO müssen dafür folgende Kriterien erfüllt sein:

- ein **maschinengestütztes** System,
- ausgelegt auf einen in unterschiedlichem Grade **autonomen Betrieb**,
- das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann,

- mit **Ableitung** expliziter oder implizierter Ziele, wie Ausgaben erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können. Diese Ausgaben können z.B. Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen sein.



PRAXIS-TIPP

Unternehmen und Behörden sollten immer zuerst prüfen, ob sie tatsächlich ein KI-System einsetzen und die Vorgaben aus der KI-VO einschlägig sein können. Dies sollten Sie als Datenschutz- oder KI-Bbeauftragter, KI-Manager oder KI-Berater initiieren. Liegt kein KI-System vor, ist die Prüfung nach der KI-VO auch schon beendet. →

Der Anwendungsbereich der KI-VO ist in diesem Fall eröffnet. Denn die Software dient nicht nur dazu, bereits eingesprochene Stimmufnahmen zusammenzusetzen. Vielmehr soll sie für den Podcast gänzlich neue Toninhalte mithilfe der Stimme des Mitarbeiters erzeugen.

2. Liegen verbotene KI-Praktiken vor?

Ist die KI-VO anwendbar, folgt Prüfschritt 2: Grundsätzlich dürfen bei einem Podcast keine verbotenen KI-Praktiken im Sinne des Art. 5 KI-VO zum Einsatz kommen. Dazu zählen z.B. KI-Systeme mit Techniken der unterschwelligen Beeinflussung oder absichtlich manipulativen oder täuschenden Techniken, die zu (ansonsten nicht getroffenen) Entscheidungen mit einem (hinreichend wahrscheinlichen) erheblichen Schaden für Personen führen können (Art. 5 Abs. 1 Buchst. a KI-VO).

Das bedeutet in unserem Fall: Ein Mensch muss den KI-generierten Inhalt des Podcasts überprüfen. So dürfen die Toninhalte beispielsweise nicht Verwendung finden, um den Zuhörerinnen und Zuhörern Anreize für ein potenziell schädliches Verhalten zu geben.

Dies kann beispielsweise bei einer Werbung für gefährliche Produkte oder bei einer Verherrlichung selbstgefährdender Handlungen gegeben sein.

3. Besteht ein Hochrisiko-KI-System oder 4. ein KI-System mit begrenztem Risiko?

Kommen keine verbotenen KI-Praktiken zum Einsatz, dann ist zu prüfen, ob die Voraussetzungen für ein Hochrisiko-KI-System nach Art. 6 KI-VO bei dem Podcast erfüllt sein könnten. Unter die Hochrisiko-KI-Systeme fallen gemäß Art. 6 Abs. 2 KI-VO in Verbindung mit Anhang III KI-VO z.B. KI-Systeme,

- die biometrische Daten für bestimmte Zwecke (beispielsweise zur Fernidentifizierung, Kategorisierung und Emotionserkennung) verarbeiten (Anhang III Nr. 1 Buchst. a–c KI-VO) oder

- der Beobachtung und Leistungsbeurteilung am Arbeitsplatz dienen (Anhang III Nr. 4 Buchst. b KI-VO).

Bei der Erstellung und Veröffentlichung eines Podcasts dürften die Kriterien für ein Hochrisiko-KI-System regelmäßig nicht vorliegen. Damit haben wir es mit einem KI-System mit einem begrenzten Risiko zu tun.



PRAXIS-TIPP

Die Vorgaben für den Einsatz von Hochrisiko-KI-Systemen müssen derzeit noch nicht umgesetzt werden, siehe url.me/r7Y4V3. Dennoch sollten Sie sich als Ansprechperson für KI-Themen frühzeitig mit den Regelungen auseinandersetzen. Eine Prüfung kann bereits jetzt sinnvoll sein.

5. Welche Pflichten bestehen?

Folgende Vorgaben bestehen in Bezug auf ein KI-System mit begrenztem Risiko bei der Erstellung eines Podcasts:

Transparenz

Im Hinblick auf mit KI erstellte Audioinhalte sind gemäß der aktuellen Fassung der KI-VO im Allgemeinen ab dem 02.08.2026 Transparenzpflichten umzusetzen (Art. 50 Abs. 2 und 4 KI-VO), bei bestehenden Inhalten gilt dies für Anbieter erst ab dem 02.12.2026 (AI Omnibus, Stand 16.06.2026). Synthetische Audioinhalte müssen grundsätzlich „in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar“ sein. Im Hinblick auf die Transparenzpflicht bestehen Ausnahmen, die jedoch nur für eng definierte Fälle greifen. (Zu den Details siehe den Beitrag S. 6–8.)

KI-Kompetenz

Schon heute gilt die gesetzliche Pflicht zur Schaffung eines ausreichenden Maßes an KI-Kompetenz bei den Beschäftigten sowie anderen Personen, die KI-Systeme im Auftrag des Unternehmens oder der Behörde nutzen bzw. betreiben (Art. 4 KI-VO). Diejenigen, die

aktiv mit dem Einsatz betraut sind, sollten also geschult sein. Der KI-Beauftragte oder eine Person in vergleichbarer Position sollte dies überwachen.



PRAXIS-TIPP

Eine ausreichende KI-Kompetenz muss grundsätzlich bei allen Beschäftigten nachweisbar sein, die KI zu dienstlichen Zwecken nutzen. Es empfiehlt sich daher, KI-Schulungen direkt im Onboarding der Beschäftigten durchzuführen.

In unserem Fall lautet also das Ergebnis: Für die Erstellung des Podcasts kommt ein KI-System mit begrenztem Risiko zum Einsatz. Damit sind die Transparenzpflichten aus der KI-VO zu erfüllen (Kennzeichnung KI-generierter Inhalte). Außerdem müssen die Personen, die mit dem KI-System arbeiten, KI-Kompetenz nachweisen können.

Empfehlung: Dokumentation

Grundsätzlich empfiehlt es sich, die durchgeführte Prüfung des eingesetzten KI-Systems – vor allem die Risikoklassifizierung – intern zu dokumentieren. Dies kann Nachweiszwecken dienen und helfen, den Überblick über die eingesetzte KI und ihre Anforderungen zu behalten.

Rechtsgrundlage für die Datenverarbeitung

Neben der KI-rechtlichen Bewertung muss auch die datenschutzrechtliche Rechtmäßigkeit bei der Erstellung des Podcasts mithilfe des KI-Systems sichergestellt sein.

Für die erstmalige Stimmabgabe und mögliche Erprobung der Funktionalität (sowie gegebenenfalls Verbesserung der späteren KI-Stimme) kommt grundsätzlich die Einwilligung des betroffenen Mitarbeiters nach § 26 Abs. 2 Bundesdatenschutzgesetz (BDSG) in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) bzw. § 26 Abs. 3 BDSG in Verbindung mit Art. 9 Abs. 2 Buchst. a DSGVO in Betracht.

Letztgenannte Rechtsgrundlage könnten Unternehmen vorsorglich heranziehen, sofern die Stimme der Person als „biometrisches Datum“ betrachtet wird und somit besondere Kategorien personenbezogener Daten berührt wären.

Allerdings wird die Freiwilligkeit der Einwilligung im Beschäftigungskontext oft kritisch betrachtet. Deshalb müsste sichergestellt sein, dass den Mitarbeitenden, die eine Einwilligung verweigern, keine Nachteile drohen. Zudem sind die weiteren Anforderungen an eine wirksame Einwilligung (z.B. Informiertheit, Nachweisbarkeit) zu berücksichtigen.



ACHTUNG

Unternehmen sollten die Stimme nicht für andere Anwendungsfälle außerhalb der erteilten Einwilligung (z.B. für Anrufbeantworter) oder für das weitere Training des eingesetzten KI-Systems nutzen.

Selbst wenn die Einwilligung des Mitarbeiters das Training der KI mit seiner Stimme ausdrücklich umfasst, bestehen datenschutzrechtliche Risiken im Hinblick auf die Geltendmachung von Betroffenenrechten. So kann z.B. eine Löschung – die bei einem späteren Widerruf der Einwilligung erforderlich ist – eine große technische Herausforderung darstellen, wenn das KI-System mit Daten der betroffenen Person trainiert wurde.

Unter der Annahme, dass mit der Stimme keine besonderen Datenkategorien verarbeitet werden, könnte die Datenverarbeitung alternativ mit einem gesonderten Vertrag gerechtfertigt werden, den das Unternehmen speziell für den Podcast mit dem Mitarbeiter abschließt. Rechtsgrundlage wäre in diesem Fall Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO. Dieser Artikel sieht kein Widerrufsrecht vor.

Es ist in diesem Fall jedoch dringend zu raten, ebenfalls auf eine hinreichende Frei-

willigkeit zu achten und den Vertrag – auch zivilrechtlich – sorgfältig zu prüfen.

Datenschutzrechtliche Prüfung des KI-Systems

Im Rahmen der datenschutzrechtlichen Bewertung ist zudem relevant, inwiefern externe Dienstleister einbezogen sind und welche Rolle diese bei der Datenverarbeitung einnehmen. In der Regel stellt die Bereitstellung eines KI-Systems für andere Unternehmen eine Auftragsverarbeitung nach Art. 28 DSGVO dar und ist durch einen entsprechenden Datenschutzvertrag abzusichern.

Bei vielen gängigen KI-Modellen ist die Verarbeitung personenbezogener Daten in einem Drittland der Regelfall. Hierbei gilt es, die dafür erforderlichen Vereinbarungen bzw. Garantien zu überprüfen. Ferner müssen Unternehmen die Grundsätze für die Verarbeitung personenbezogener Daten (in Art. 5 Abs. 1 DSGVO) sicherstellen, wie z.B. die Umsetzung der

Prinzipien der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) und Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO). Vorzunehmen sind außerdem eine datenschutzrechtliche Dokumentation im Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) sowie vor dem Einsatz des KI-Systems eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO).



PRAXIS-TIPP

Bei KI-Systemen mit einer Verarbeitung personenbezogener Daten müssen auch die datenschutzrechtlichen Anforderungen geprüft werden. Der bzw. die Datenschutzbeauftragte ist daher rechtzeitig einzubeziehen.



Conrad S. Conrad, Volljurist, ist Senior Berater Datenschutz und Elena Folkerts, M.A., Senior Beraterin Datenschutz sowie zertifizierte KI-Compliance-Beauftragte. Beide sind tätig bei der Datenschutz nord GmbH in Hamburg.

Anforderung/Fragestellung	Ja	Nein
Kommt ein KI-System (im Sinne des Art. 3 Nr. 1 KI-VO) zum Einsatz?	☐	☐
Fällt der Einsatz des KI-Systems unter die verbotenen KI-Praktiken (aus Art. 5 KI-VO)?	☐	☐
Fällt der Einsatz des KI-Systems unter die Hochrisiko-KI-Systeme (nach Art. 6 KI-VO)?	☐	☐
Weist das Unternehmen oder die Behörde auf den Einsatz von KI zur Erstellung der Audioinhalte hin (Art. 50 Abs. 2 KI-VO für Anbieter, Art. 50 Abs. 4 KI-VO für Betreiber)?	☐	☐
Wurden die Beschäftigten, die das KI-System einsetzen, im Hinblick auf die Nutzung und den Betrieb von KI-Systemen sensibilisiert?	☐	☐
Empfehlung: Wurde die Prüfung/Risikoklassifizierung des KI-Systems dokumentiert?	☐	☐
Ist auch die datenschutzrechtliche Rechtmäßigkeit sichergestellt, indem eine Einwilligung der betroffenen Person (gemäß den datenschutzrechtlichen Vorgaben) eingeholt wird oder ein angemessener Vertrag als Grundlage dienen kann?	☐	☐
Wird die betroffene Person über die Datenverarbeitung hinreichend transparent informiert (Art. 13 DSGVO)?	☐	☐
Falls ein externer Dienstleister das KI-System bereitstellt: Besteht ein Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO)?	☐	☐
Sind die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO) umgesetzt?	☐	☐
Sind eine datenschutzrechtliche Dokumentation (Art. 30 DSGVO) und eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) erfolgt?	☐	☐

Anforderungen bei der Nutzung echter Stimmen für KI-generierte Inhalte. Die Checkliste finden Sie zum direkten Download unter url.me/CSwYM5.



Vor dem Einsatz KI-gestützter Programmierassistenten sind wesentliche Fragen zu klären

Bild: KI-generiert durch den Autor



WICHTIG

Claude Code und Codex basieren auf Cloud-KI. Die KI läuft also auf den Servern von Anthropic und OpenAI. Der Coding-Agent schickt alle Daten zum jeweiligen Anbieter. Alle Ergebnisse werden in der Cloud produziert und dann an das System des Nutzers zurückgeschickt.

Praxisleitfaden zu zwei weitverbreiteten Programmierassistenten

Claude Code und Codex sicher im Unternehmen nutzen

KI-gestützte Coding-Assistenten wie Claude Code (Anthropic) und Codex (OpenAI) halten in immer mehr Unternehmen Einzug – oft schneller, als Richtlinien, Schulungen und Governance-Strukturen folgen können. KI-Beauftragte sollten den Einsatz rahmen, bevor er unkontrolliert wächst.

Dieser Artikel konzentriert sich auf praxisnahe Empfehlungen, die sich leicht umsetzen lassen.

Was sind Claude Code und Codex?

Beide Plattformen sind agentenbasierte Coding-Assistenten. Sie gehen weit über einfache Code-Vervollständigung hinaus:

- **Claude Code** von Anthropic läuft direkt im Terminal und kann eigenständig Dateien lesen, schreiben, Befehle ausführen und ganze Entwicklungsaufgaben übernehmen – auf Anweisung des Nutzers, aber mit erheblichem Handlungsspielraum.
- **Codex** von OpenAI funktioniert ähnlich: Es analysiert Codebasen, führt Tests aus und schlägt Änderungen vor.

Der entscheidende Unterschied zu einfachen Chat-KI-Tools: Diese Plattformen handeln selbstständig und antworten nicht nur auf Fragen. Sie können Dateien überschrei-

ben, Skripte ausführen und auf Datenbanken zugreifen – wenn die Zugriffsrechte entsprechend eingestellt sind und keine Sicherheitsvorkehrungen dies verhindern.

Grundlegende Risiken

Die wichtigsten Risiken bei der Nutzung von Coding-Agenten aus der Cloud in der Praxis:

Unbeabsichtigte Datenweitergabe:

Entwickler fügen routinemäßig Codeausschnitte oder Konfigurationsdateien als Kontext in ihre Anfragen ein. Darin können Personendaten, API-Schlüssel (API: Programmierschnittstelle) oder sensible Informationen stecken.

Unkontrollierte Aktionen im System:

Agentenbasierte Tools wie Claude Code können eigenständig Code ausführen, Dateien löschen oder Systemkonfigurationen ändern. Dies kann größere Schäden verursachen, wenn solche Werkzeuge unkonfiguriert zum Einsatz kommen.

Einschleusung von Schadcode: Liest ein KI-Tool externen Code oder Webinhalte, können darin Anweisungen versteckt sein, die das Verhalten des Assistenten manipulieren.

Unkontrollierte Datenweitergabe: Je nach Vertrag und Konfiguration kann der KI-Anbieter Eingaben (und Ausgaben) auswerten oder zum KI-Training verwenden.

Blindes Vertrauen: Nutzende neigen dazu, KI-generierten Code ohne ausreichende Prüfung zu übernehmen. Fehler, Sicherheitslücken und lizenzrechtlich problematischer Code können so unbemerkt ins Produkt gelangen.

Eingabebeschränkungen für Prompts

Klare Regeln, was die Mitarbeitenden in Claude Code oder Codex eingeben dürfen, verhindern den Großteil der Risiken. Beim Einsatz lokaler Agenten wie z.B. Hermes Agent hingegen können diese Beschränkungen entfallen.

Kritische Daten in KI-Prompts

Folgende Daten sollten nicht in Prompts landen, die zu Dritten geschickt werden:

- personenbezogene Daten (Kundennamen, E-Mail-Adressen etc.)
- Zugangsdaten (Passwörter, API-Keys, Zertifikate, Tokens)
- interne Systemarchitektur (z.B. Datenbankschemata, Netzwerkpläne)
- vertragliche Daten (z.B. Kundendaten aus dem CRM-System, Angebote)
- Quellcode mit Geschäftsgeheimnissen (Algorithmen, die einen Wettbewerbsvorteil darstellen)

