WISSEN
TECHNIK
LEIDENSCHAFT

AI Act Checklist und Codes of Conduct

Christof Wolf-Brenner

Technische Universität Graz
Institute of Interactive Systems and Data Science
Sandgasse 36
A 8010 Graz

13.05.2024

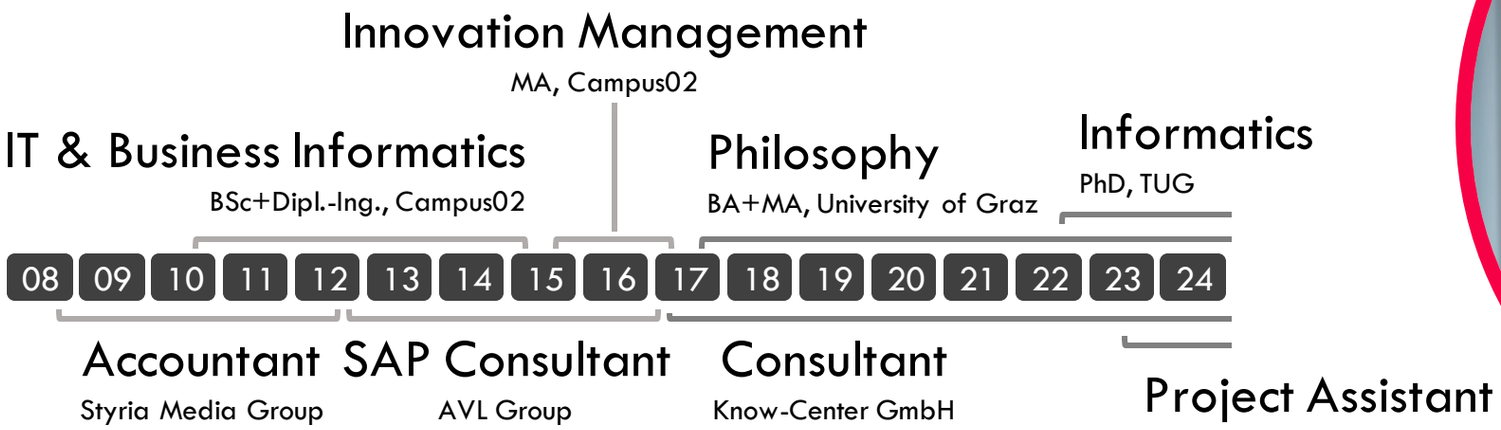
Kontakt: c.wolf-brenner@tugraz.at

Agenda

- 09:00-09:30: Begrüßung, einleitende Worte zum Setting
- 09:30-10:00: Vorstellung identifizierter KI-Use Cases in KMU
- 10:00-11:30: Vorstellung AI Act Checklist & Leitfragen Codes of Conduct
- 11:30-12:00 Feedback & Abschluss

Dipl.-Ing. Christof Wolf-Brenner, MA

PhD Student / Project Assistant



Kontakt: c.wolf-brenner@tugraz.at

Zum Projekt

- Innovationsvorhaben der TUG über den DIH Süd
- September 2023 - Juni 2024
- Ziele
  1. Identifikation von Beispiel-Cases aus dem KMU Umfeld in denen KI eingesetzt wird bzw. der AI Act relevant ist
  2. Checklist für KMU die es erlaubt, festzustellen ob der AI Act angewendet werden muss (erster Indikator)
  3. Leitfragen zur Erstellung eines Verhaltenskodex (Code of Conduct)

Zum Projekt

1. **Erhebung des Status Quo:** Durchführung von bilateralen Vorgesprächen mit regionalen KMUs zur Erfassung bestehender KI-Anwendungen und zum Verständnis spezifischer Bedürfnisse und Herausforderungen.
2. **Entwicklung von Tools:** Erarbeitung einer Checkliste und Leitfragen für Codes of Conduct basierend auf der Erhebung und existierender Literatur
3. **Pilotierung:** Durchführung eines Workshops zur Vorstellung und Validierung der entwickelten Tools.
4. **Finalisierung und Veröffentlichung:** Abschluss der Erstellung der Checkliste und der Leitfragen und deren Veröffentlichung unter einer Creative Commons Lizenz zur freien Nutzung.

WISSEN
TECHNIK
LEIDENSCHAFT

Beispiel KI-Use-Case aus KMU

Christof Wolf-Brenner

Technische Universität Graz
Institute of Interactive Systems and Data Science
Sandgasse 36
A 8010 Graz

13.05.2024

Kontakt: c.wolf-brenner@tugraz.at

U1: Nutzung von Sprachmodellen (LLMs) zur Generierung und Dokumentation von Programmcode

U1: Nutzung von Sprachmodellen (LLMs) zur Generierung und Dokumentation von Programmcode

In kleinen und mittleren Unternehmen (KMU) wird Künstliche Intelligenz (KI) zunehmend für die Optimierung von Softwareentwicklungsprozessen eingesetzt. Ein zentraler Use Case in diesem Kontext ist die auto-matische Generierung von Programmcode basierend auf nutzer-generierten Daten wie Softwarefunktionsbeschreibungen, Code-Beispielen oder Anforder-ungsspezifikationen. Durch den Einsatz von modernen Sprachmodellen, wie zum Beispiel ChatGPT oder GitHub Copilot, werden aus den eingegebenen Beschreibungen direkt umsetzbare Code-Segmente erstellt.

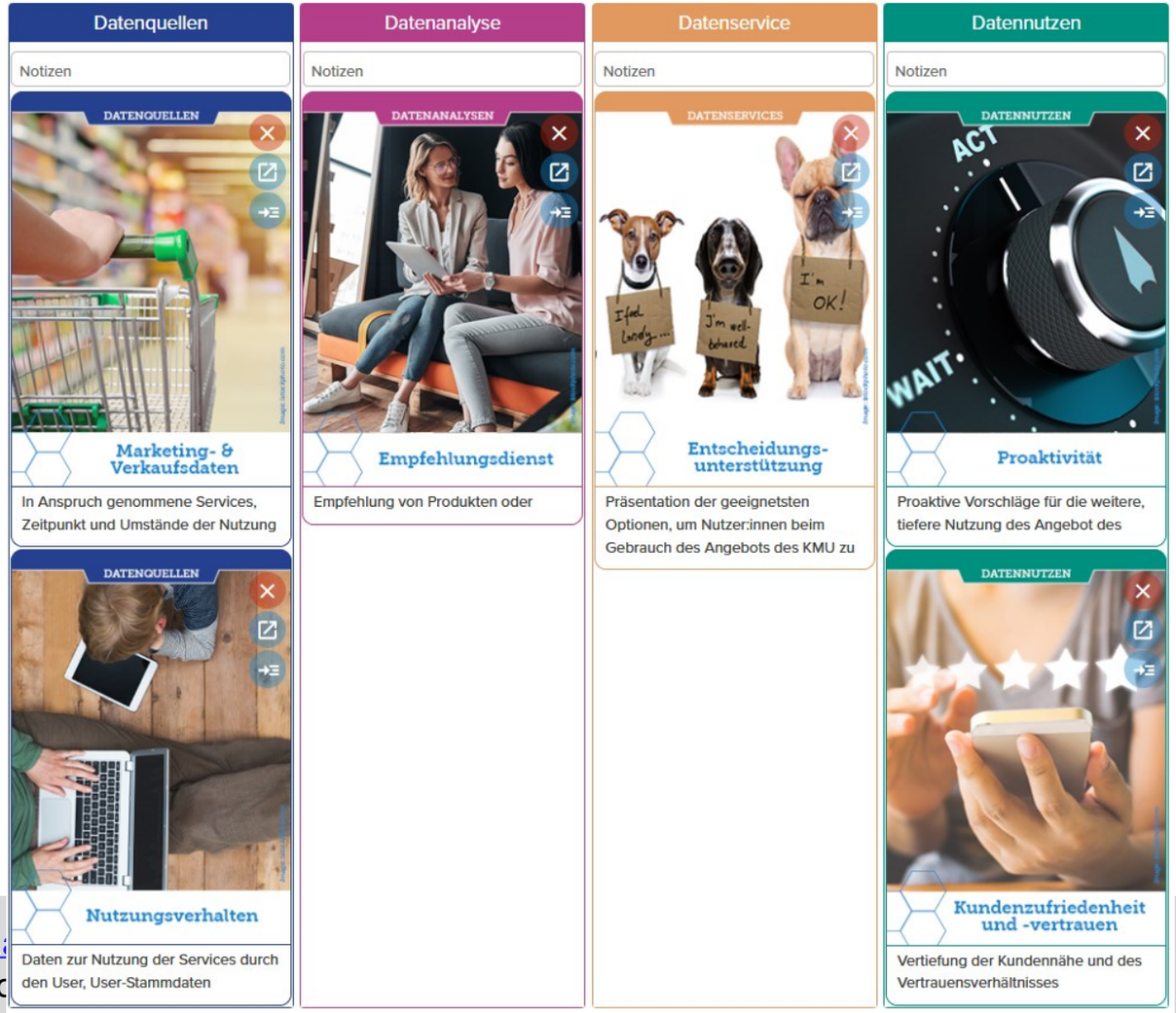
U1: Nutzung von Sprachmodellen (LLMs) zur Generierung und Dokumentation von Programmcode

Diese Vorgehensweise ermöglicht es, dass Programmierer:innen, in der Regel durch einfaches Kopieren des generierten Codes aus einer Oberfläche oder einem Chat-Fenster, diesen direkt in ihre Entwicklungsumgebung integrieren können. Der primäre Nutzen dieses Ansatzes liegt in der erheblichen Zeitersparnis: Aufwendige Recherchen und das Ausformulieren und Dokumentieren von Standardfunktionen, die sonst oftmals manuell von Entwickler:innenn durchgeführt werden müssen, werden durch dieses KI-gestützte Vorgehen teilautomatisiert. Dadurch kann die Effizienz in den Softwareentwicklungsprozesse gesteigert werden.

U1: Nutzung von Sprachmodellen (LLMs) zur Generierung und Dokumentation von Programmcode

1. **Risikoklassifizierung**: Abhängig von der Art und Weise, wie die generierte Software verwendet wird, könnte sie in eine unterschiedliche Risikokategorien des AI Act fallen. Software, die kritische Infrastrukturen unterstützt, könnte beispielsweise als hochriskant eingestuft werden, was strengere Regulierungen nach sich zieht.
2. **Transparenz und Dokumentation**: Der AI Act legt großen Wert auf Transparenz gegenüber den Nutzern. Dies ist insbesondere relevant, wenn die Software eigenständig Entscheidungen ableitet oder Prozesse automatisiert, die für die Gesellschaft von Bedeutung sind.
3. **Datenschutz und Datensicherheit**: Bei der Nutzung von nutzergenerierten Daten zur Code-Generierung müssen KMU die Datenschutzvorschriften beachten, insbesondere die Datenschutz-Grundverordnung (DSGVO) und die spezifischen Anforderungen des AI Act hinsichtlich der Datensammlung und -verarbeitung.
4. **Haftung**: Der AI Act adressiert auch Fragen der Haftung für Schäden, die durch KI-Systeme verursacht werden. KMU müssen sich der potenziellen Haftungsrisiken bewusst sein, die entstehen können, wenn die von KI generierte Software fehlerhaft ist oder Schaden verursacht.

U2: Cross- und Upselling-Empfehlungen auf Basis von Nutzungsverhalten



Kontakt: c.wolf-brenner@tugraz.
AI Act Checklist und Codes of Co

U2: Cross- und Upselling-Empfehlungen auf Basis von Nutzungsverhalten

Ein zentraler Use Case in KMU ist die Implementierung von KI-basierten Empfehlungsdiensten, die auf Analysen von Marketing- und Verkaufsdaten sowie dem Nutzungs- bzw. Kaufverhalten von Kund:innen beruhen.

Diese Daten umfassen Informationen über in Anspruch genommene Services, den Zeitpunkt und die Umstände der Nutzung sowie detaillierte Daten zum Nutzungsverhalten der Services oder Produkte durch die User, einschließlich der User-Stammdaten. Die Analyse dieser Datensätze ermöglicht es, individuell zugeschnittene Empfehlungen für weiterführende Produkte oder Services zu generieren. Der Fokus liegt hierbei auf Cross- oder Upselling-Potenzialen, die sich aus der bisherigen Interaktion des Kunden mit dem Angebot des KMU ergeben.

U2: Cross- und Upselling-Empfehlungen auf Basis von Nutzungsverhalten

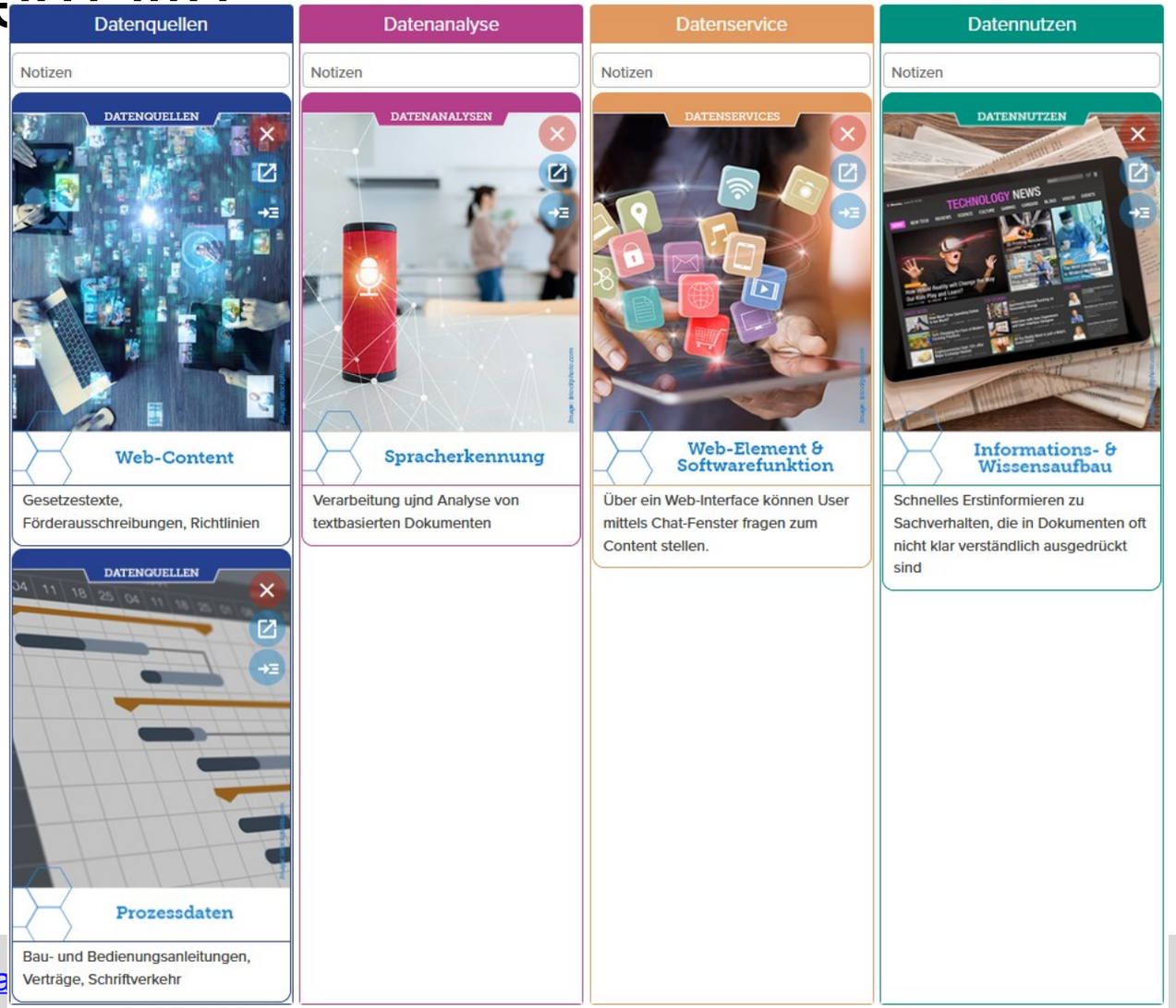
Die KI-gestützte Entscheidungsunterstützung präsentiert den Nutzern die für sie geeignetsten Optionen, um sie bei der Auswahl weiterführender Produkte oder Services zu unterstützen. Diese Art der personalisierten Empfehlung zielt darauf ab, Kunden proaktive Vorschläge zu unterbreiten, die auf ihre individuellen Bedürfnisse und bisherigen Erfahrungen zugeschnitten sind.

Der Nutzen dieses Ansatzes erstreckt sich weiters auf die Vertiefung der Kundennähe und des Vertrauensverhältnisses. Kunden fühlen sich verstanden und wertgeschätzt, wenn ihre Bedürfnisse und Präferenzen antizipiert werden, was letztendlich zu einer stärkeren Kundenbindung und einem erhöhten Kundenwert führt.

U2: Cross- und Upselling-Empfehlungen auf Basis von Nutzungsverhalten

1. **Transparenzanforderungen:** Der AI Act legt besonderen Wert auf Transparenz gegenüber den Nutzern. Für KMU bedeutet dies, dass sie klar kommunizieren müssen, wenn ein KI-System Empfehlungen generiert. Kunden müssen darüber informiert werden, dass ihre Daten von einem KI-System verarbeitet werden, um personalisierte Empfehlungen zu erstellen. Dies umfasst auch Informationen darüber, wie diese Empfehlungen zustande kommen.
2. **Datenschutz und Datennutzung:** Die Verarbeitung persönlicher Daten durch KI-Systeme muss den Datenschutzvorschriften der EU, insbesondere der Datenschutz-Grundverordnung (DSGVO), entsprechen. KMU müssen sicherstellen, dass die Datenerhebung, -verarbeitung und -nutzung für KI-gestützte Empfehlungssysteme die gesetzlichen Anforderungen erfüllt.
3. **Qualitäts- und Sicherheitsanforderungen:** Der AI Act verlangt, dass KI-Systeme sicher und zuverlässig sind. KMU müssen demnach gewährleisten, dass die von KI-Modellen unterstützte Software robust, sicher und frei von unerwünschten Verzerrungen (Bias) ist, um Diskriminierung zu vermeiden und die Integrität der Empfehlungen zu sichern.

U3: Erklärungs- und Kommunikationssystem für Spezialsachverhalte



U3: Erklärungs- und Kommunikationssystem für Spezialsachverhalte

KMU setzen verstärkt auf KI, um die Verarbeitung und Analyse von textbasierten Dokumenten zu optimieren. Ein innovativer Use Case in diesem Bereich ist die Entwicklung von Systemen, die es Nutzern ermöglichen, über ein Chat-Fenster auf einer Webseite gezielte Fragen zu spezifischen Inhalten zu stellen. Diese Anwendungsfälle beziehen sich häufig auf eine Vielzahl von Dokumententypen, darunter beispielsweise externe Daten wie Gesetzestexte, Förderausschreibungen, Richtlinien etc. sowie interne wie Bau- und Bedienungsanleitungen, Verträge, Schriftverkehr und viele mehr.

U3: Erklärungs- und Kommunikationssystem für Spezialsachverhalte

In der Regel werden aktuell hierbei Chatbots auf Basis von externen Large Language Models eingesetzt. Nutzer können dann spezifische Fragen stellen, woraufhin basierend auf den Informationen, die in den zugrunde liegenden Dokumenten gefunden wurden, Antworten generiert werden.

Der primäre Nutzen dieses Ansatzes liegt im schnellen Informations- und Wissensaufbau bei Nutzer:innen. Indem komplexe Sachverhalte, die in Dokumenten oft in fachspezifischer Sprache verfasst sind, in einer verständlichen Form präsentiert werden, können Nutzer sich effizient zu verschiedenen Themen erstinformieren. Dies verbessert nicht nur die Zugänglichkeit und Verständlichkeit von wichtigen Informationen, sondern trägt auch dazu bei, die Effizienz interner Prozesse zu steigern, da Mitarbeiter weniger Zeit mit der Suche und Interpretation von Informationen verbringen müssen.

U3: Erklärungs- und Kommunikationssystem für Spezialsachverhalte

- **Transparenz und Offenlegung:** KMU müssen die Nutzung von KI-Systemen gegenüber den Nutzern klar kommunizieren. Diese müssen zumindest darüber informiert werden, dass ihre Anfragen von KI-Systemen bearbeitet werden.
- **Datenqualität und -management:** Die Grundlage für die Zuverlässigkeit von KI-Systemen bildet die Qualität der Trainingsdaten. KMU müssen sicherstellen, dass die verwendeten Daten korrekt sind, um Fehlinformationen zu vermeiden. Dies ist besonders wichtig, da die Genauigkeit der KI-basierten Antworten direkte Auswirkungen auf die Entscheidungsfindung der Nutzer haben kann.
- **Risikomanagement:** Die Bewertung und das Management von Risiken, die mit dem Einsatz von KI verbunden sind, sind von höchster Bedeutung. KMU müssen potenzielle Risiken, die sich aus der Bereitstellung von durch externe KI gestützte Diensten ergeben, identifizieren und Maßnahmen ergreifen, um diese Risiken zu minimieren.

WISSEN
TECHNIK
LEIDENSCHAFT

AI Act Checklist

Christof Wolf-Brenner

Technische Universität Graz
Institute of Interactive Systems and Data Science
Sandgasse 36
A 8010 Graz

13.05.2024

Kontakt: c.wolf-brenner@tugraz.at

Ziele der AI Act Checklist

- Beantwortung der Frage: Sollte ich mich mit dem AI Act tiefergehend beschäftigen?
- Systembasierte Betrachtung
- Möglichst selbsterklärend, schnell, intuitiv und einfach anwendbar
- Ist keine und ersetzt keine Rechtsberatung

Kernbereiche /-fragen

- Ist das betrachtete System ein KI-System iSd AI Act?
- Wird das KI System auf eine Art und Weise verwendet, sodass er AI Act schlagend werden könnte?
- Wird das KI System im Geltungsbereich des AI Act verwendet?
- Ist die Nutzung des KI-System vom AI Act ausgenommen?

Testszenarien

U1: Nutzung von Sprachmodellen (LLMs) zur Generierung und Dokumentation von Programmcode

- Mitarbeiter eines Unternehmens verwenden ChatGPT zur Generierung/Dokumentation/Korrektur von Programmcode

U2: Cross- und Upselling-Empfehlungen auf Basis von Nutzungsverhalten

- Ein Unternehmen nutzt ein von Dritten für Sie entwickeltes KI-System auf Basis von Machine Learning, das Kunden auf der Webseite weitere Produkte/Services zum Kauf vorschlägt.

U3: Erklärungs- und Kommunikationssystem für Spezialsachverhalte

- Ein Unternehmen vereinfacht das Verstehen seiner Bedienungsanleitung durch Upload des Dokumentes und Chat mit ChatGPT.

WISSEN
TECHNIK
LEIDENSCHAFT

Code of Conduct Template

Christof Wolf-Brenner

Technische Universität Graz
Institute of Interactive Systems and Data Science
Sandgasse 36
A 8010 Graz

13.05.2024

Kontakt: c.wolf-brenner@tugraz.at

Art 69 AI Act

- The Commission and the Member States shall encourage and facilitate the **drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems** of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.
- The Commission and the Board shall encourage and facilitate the **drawing up of codes of conduct intended to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams** on the basis of clear objectives and key performance indicators to measure the achievement of those objectives.
- Codes of conduct may be drawn up **by individual providers of AI systems or by organisations representing them or by both**, including with the involvement of users and any interested stakeholders and their representative organisations. Codes of conduct **may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems**.
- The Commission and the Board shall take into account the specific interests and needs of the small-scale providers and start-ups when encouraging and facilitating the drawing up of codes of conduct.

Feedback aus Interviewstudie zu CoC

Vertrauensbildung und Markenstärkung

- **Frühzeitige Etablierung:** Durch die frühzeitige Ausarbeitung eines Ethikkodexes durch Mitgründer werden Unternehmenswerte fest verankert und transparent kommuniziert.
- **Employer Branding:** Ein klar definierter Verhaltenskodex verbessert das Employer Branding, indem er zeigt, dass das Unternehmen sinnvolle und ethisch fundierte Arbeit leistet.
- **Vertrauensförderung:** Der Kodex dient als Beweis für die Glaubwürdigkeit und Zuverlässigkeit des Unternehmens, stärkt das Vertrauen bei Kunden und Partnern.

Feedback aus Interviewstudie zu CoC

Regulatorische und ethische Compliance

- **Über gesetzliche Anforderungen hinaus:** Der Kodex setzt Standards, die oft über die gesetzlichen Mindestanforderungen hinausgehen, und adressiert spezifische ethische Herausforderungen.
- **Blacklisting von Use Cases:** Bestimmte Anwendungsfälle, die als unethisch oder problematisch angesehen werden, KÖNNEN explizit ausgeschlossen werden.

Feedback aus Interviewstudie zu CoC

Operative und strategische Vorteile

- **Leitfaden für tägliche Operationen:** Der Kodex kann als konkreter Leitfaden für Entscheidungen und Handlungen im täglichen Betrieb dienen.
- **Basis für Zertifizierungen:** Der Kodex kann als Grundlage für branchenspezifische Gütesiegel dienen, was die Marktposition stärken und Wettbewerbsvorteile schaffen kann.

Feedback aus Interviewstudie zu CoC

Kommunikation und Transparenz

- **Interne und externe Klarheit:** Der Kodex schafft Klarheit über die Unternehmenswerte sowohl intern bei Mitarbeitern als auch extern bei Kunden und Partnern.
- **Instrument der Kommunikation:** Erklärt verantwortungsvollen Umgang mit Daten und Technologie und wirkt präventiv gegen Missbrauch und Missverständnisse.

Feedback aus Interviewstudie zu CoC

Herausforderungen bei der Umsetzung

- **Ressourcenaufwand:** Die Entwicklung und Pflege eines Kodex kann insbesondere für KMU ressourcenintensiv sein.
- **Durchsetzung und Compliance:** Die Einhaltung des Kodex muss regelmäßig überprüft und durch interne Prozesse gesichert werden.

Feedback aus Interviewstudie zu CoC

Fazit

- **Das Verfassen eines Code of Conduct ist nur der Anfang.**
- **Wer seinen Code of Conduct ernst nimmt, muss zusätzlich Prozesse implementieren, die die Überwachung der Einhaltung, Sanktionierung von Verstößen und Adaptierung des CoC beinhalten.**