AI Guideline Bingo 1.3



KI-Richtlinien regeln die **Nutzung von KI-Systemen** in Organisationen. Was genau geregelt wird und wie verbindlich, wie detailliert und welche **Perspektiven** eher in einer Richtlinie auftauchen, einer KI-Strategie, einzelnen Nutzungskonzepten oder einer Betriebsvereinbarung - das variiert stark. Gesetze gelten ohnehin, aber es braucht **Orientierung**.

Weniger ist mehr - eine Richtlinie, die nicht gelesen wird bleibt wirkungslos. Gleichzeitig gilt es den **Sicherheitsbedürfnissen** von Personen und Organisationen gerecht zu werden und gleichzeitig das **Spielfeld für Innovationen** zu definieren. Sprechen wir darüber?

Prozesse

- **Zugang**
  Wer darf auf welche KI-Systeme
  (im Sinne von sicher und fair) zugreifen?
- **Erprobung**
  Was ist ohne Freigabe möglich?
- **Aufsicht**
  Welche Kontrollmechanismen gibt es?
  Wie stellen wir Wirksamkeit fest?
- **Selbstbedienung**
  Was können Nutzende allein? Wo sind Grenzen?
- **Freigabe**
  Wie kommt man an neue KI-Systeme?
- **Feedback**
  Wie lernt die Organisation aus den Erfahrungen mit KI-Systemen?
- **Klärung**
  Richtlinie unklar? Wer klärt?
- **Eskalation**
  Was geschieht bei Verstoß?
- **Mitbestimmung**
  Gibt es einen Betriebsrat? Wie einbezogen?

Grundlagen

- **Scope**
  Um welche Systeme geht es?
- **Positivliste**
  Welche KI-Systeme sind zulässig?
- **Eingaben**
  Welche Daten dürfen hinein?
  (Personendaten, Geschäftsgeheimnisse, Urheberrecht)
- **Zweck**
  Was darf und was darf nicht?
  (Verbotene Praktiken, Menschen bewerten, Deep Fakes...)
- **Ausgaben**
  Wie gehen wir mit Outputs verantwortungsvoll um?
  (Prüfen, Kennzeichnung, Urheberrecht)

Verantwortung

- **Organisation**
  Wer verantwortet was?
- **AI-Literacy**
  Was ist erforderlich? Zwingende Zugangsvoraussetzung?
- **Sicherheit**
  Welche Sicherheits- und Awareness-Maßnahmen sind erforderlich?
- **Autonomie**
  Wie viel Autonomie bekommen Prozesse und Agenten wann?
- **Hochrisiko-Fälle per KI-Verordnung**
  Ausschließen oder nicht?
- **Audits**
  Was machen Nutzende? Gibt es Prüfungen? Wie?
- **Systemintegration**
  Sind Systeme noch getrennt bewertbar?
  Oder spricht man per MCP, CLI und API mit allen Systemen?
- **Nachhaltigkeit**
  Was fordern / bieten wir? Wie transparent sind wir?
- **Souveränität**
  Was geht wo? Verbindlich oder als Wunsch?
- **Transparenz**
  Was kennzeichnen? Mit welchen Mitteln?

Effekte

- **Kosten**
  Erfasst und zugeordnet? Wie granular?
- **Rendite**
  Wer profitiert von Freiheiten / Ersparnissen / Verbesserungen?
- **Ängste und Sorgen**
  Wie handhaben?

Daten

- **Protokolle**
  Was wird aufgehoben? Wie lang und wie geschützt?
- **Lernen**
  Darf mit unseren Daten gelernt werden? Mit welchen?
- **Privates**
  Private Nutzung von KI-Systemen?
- **Qualität**
  Was tun gegen "Garbage In / Garbage Out"?

Administration

- **Verweise**
  Welche Dokumente sind explizit zusätzlich relevant?
- **Dritte**
  Was gilt für Partner und Externe?
- **Aktualisierung der Richtlinie**
  Wie und wann entwickelt sich Systeme, Steckbriefe und die Richtlinie weiter?
- **Verbindlichkeit**
  Wer verpflichtet wen? Mit Unterschrift oder ohne? Wie wird die Guideline wirksam?