KI-Verordnung in der Umsetzung – trial and error (Teil 1)
Die KI-Verordnung (KI-VO) ist nun seit einiger Zeit in Kraft und viele Unternehmen, wenn auch bei weitem noch nicht alle, befassen sich mit der Umsetzung der daraus resultierenden Anforderungen: KI-Register erstellen, Risikoeinschätzungen vornehmen, KI-Richtlinie aufsetzen, Mitarbeiter schulen…

Doch wie setzt man ein KI-VO-Projekt um, wenn Erfahrungswerte noch fehlen?
Über mehrere Artikel hinweg wollen wir Ihnen einen Einblick in unseren Arbeitsalltag als Compliance-Berater geben, die sich auf KI-VO, Informationsschutz und Datenschutz spezialisiert haben. Anhand einer fiktiven Mandantin, in der wir unsere tatsächlichen Erfahrungen bei der Umsetzung der KI-VO über mehrere Mandanten hinweg gebündelt haben, geben wir einen Einblick in die Umsetzung der KI-VO im Unternehmen – und die Stolpersteine, die einem dabei in den Weg kullern.

Es beginnt eigentlich immer gleich
Man möchte unbedingt KI-Tools einsetzen. Dringend. Weil das machen ja jetzt alle, man erhofft sich dadurch Arbeitserleichterung, Schnelligkeit, damit Effizienz, und vielleicht sogar einen Wettbewerbsvorteil. Nachvollziehbar und absolut berechtigt.
Nur mit dem rechtlichen Rahmen hat sich noch niemand auseinandergesetzt – derweil benutzen aber die Mitarbeiter schon mal fleißig KI, im Zweifelsfall mit dem kostenlosen privaten Account, bei dem dann auch alle Daten zu Trainingszwecken verwendet werden; vielleicht auch, weil die Geschäftsleitung vom Potenzial der Technologie überzeugt ist und diese Initiative intern bereits angestoßen hat. Also:

Schritt 1 – Überblick verschaffen
Zunächst müssen wir klären: Welche KI-Tools werden genutzt? Von wem? Wofür, wie, zu welchen Zwecken? Also entwickeln wir gemeinsam mit der Mandantin eine anonyme Umfrage. Doch wie machen wir das, ohne die Mitarbeiter abzuschrecken? Schnell entsteht der Eindruck, die Mitarbeitenden hätten etwas falsch gemacht – wer gibt das schon gern zu, selbst anonym?
Daher ist es extrem wichtig, den Kontext zu setzen: Zunächst einmal stellen wir klar, was wir mit der Umfrage ganz am Ende des Weges erreichen wollen, nämlich einen Überblick zu erhalten, wo im Unternehmen bereits KI-Tools eingesetzt werden und welche Wünsche an die Nutzung von KI bestehen.
Ziele der Umfrage

- Klare Rahmenbedingungen schaffen
- Rechtssichere Prozesse etablieren
- Konkrete Hilfestellungen für die Mitarbeiter bieten

Ziel ist es, den verantwortungsvollen Einsatz von KI im Unternehmen zu ermöglichen – so, dass Mitarbeiter produktiv und sicher mit diesen Tools arbeiten können. Und ganz wichtig: das Ganze muss anonym erfolgen.

Der Aha-Effekt
Soweit so gut, die Umfrage läuft, die Teilnahmequote ist recht hoch – und die Ergebnisse überraschend. Hatte man im Vorfeld noch damit gerechnet, dass so 5 – 7 Tools auf der Liste erscheinen, ist man nun plötzlich mit einer Aufzählung von über 25 KI-Tools konfrontiert, und von einigen hat man auch noch nie etwas gehört: niemand ist kreativer als der außerhalb jeglicher Vorgaben arbeitende Mitarbeiter.

Die Erkenntnis: Niemand hatte den Überblick. Weder über die Tools noch über die Einsatzzwecke. Jetzt ist Aufräumen angesagt!

Schritt 2 – Register erstellen
Bei der Sichtung der Umfrageergebnisse wird schnell klar, dass viele der genannten Tools in mehreren Abteilungen und zu unterschiedlichen Zwecken eingesetzt werden. Wir erfassen also zunächst alle

Tools in einer Liste und ordnen sie Einsatzzweck-Clustern zu, um eine bessere Übersicht zu erhalten. Die Einsatzzweck-Cluster ergeben sich dabei aus den in der Umfrage genannten Einsatzzwecken, die wir zu Überschriften verallgemeinert haben, z.B. Code-Generierung, Transkription, (Text-)Content-Generierung, Bild- und Videogenerierung, etc. In einer weiteren Spalte erfassen wir dann alle in der Umfrage genannten Detailzwecke. Dadurch können wir die Liste nach Einsatzzweck-Cluster filtern, ohne dabei Informationen zu verlieren.
Auch die Art des Zugangs erfassen wir, ebenso wie die Information, ob im genutzten Modell die durch den Nutzer eingegebenen Daten durch den Anbieter für das Training der KI genutzt werden, sowie Anbieter und den Standort der Datenspeicherung.
Das war der einfache Teil.

Schritt 3 – Risikobewertung
Mit dem KI-Register in der Hand wagen wir uns an die erste Risikoeinschätzung. Die gute Nachricht: Die KI-Verordnung liefert bereits ein Klassifikationssystem mit. Das ist hilfreich, wenn auch nicht ganz trivial:

- Verbotene Praktiken (Art. 5 KI-VO)
  (z. B. emotionserkennende Systeme am Arbeitsplatz)
- Hochrisiko-KI (Art. 6 KI-VO)
  (z. B. HR-Tools mit Einfluss auf Einstellungen/Beförderungen)
- Begrenztes Risiko (Art. 50 KI-VO)
  (z. B. Deepfakes oder interaktive KI-Systeme)
- Kein Risiko – alle in den o.g. Risikoklassen nicht enthaltenen Anwendungen

Wir ordnen die Tools und Einsatzzwecke entsprechend zu – und atmen durch: Viele der im Unternehmen genutzten Anwendungen fallen unter „kein“ oder „begrenztes Risiko“. Nur einzelne Tools im HR-Kontext müssen wir genauer prüfen. So kommen wir am Ende zu einer eigentlich ganz erfreulichen Liste und dem Schluss, dass wir auf Basis dessen, was die KI-VO vorgibt und fordert, keine Brände zu löschen haben.
Aber reicht diese Risikobetrachtung eigentlich aus?

Neue Horizonte
Natürlich nicht ganz. Denn die KI-VO definiert nur den regulatorischen Rahmen – nicht alle unternehmerischen Risiken.
Also werfen wir einen erweiterten Blick:

- Datenschutz: Werden personenbezogene Daten eingegeben? Ist eine Einwilligung erforderlich?
- Geheimnisschutz: Werden vertrauliche Dokumente analysiert? Wohin wandern diese Daten?
- Urheberrecht: Wer haftet, wenn fremde Inhalte verarbeitet werden?
- Datenstandorte: Was passiert mit meinen Daten in den USA, China oder Russland?
- Private Accounts: Sollen diese weiterhin im Unternehmenskontext erlaubt sein?

Diese Fragen sind nicht Teil der KI-VO – aber zentral für eine belastbare KI-Strategie.

Schritt 4 - Vom Risiko zur Whitelist
Jetzt heißt es: Entscheidungen treffen!

Welche KI-Systeme und Anwendungsfälle sollen künftig erlaubt sein – und welche nicht? Die Risikobewertung liefert die Grundlage, aber jetzt braucht es Klarheit und Mut zur Auswahl. Pauschale Verbote wie „Keine personenbezogenen Daten in KI-Systeme eingeben“ wirken oft lähmend und schließen sinnvolle Anwendungen, z. B. im Bereich HR, pauschal aus. Besser: Iteratives Vorgehen mit konkreten, risikoarmen Use Cases.
Wir starten bottom-up:

- KI-Systeme mit *geringem oder keinem Risiko* werden auf die *meistgenutzten* KI-Systeme reduziert
- Diese Use Cases werden konkret beschrieben und in die Richtlinie aufgenommen

Hochrisiko-Systeme – etwa im HR-Bereich – erfordern hingegen Risikominderung und sorgfältige Auswahl. Dabei helfen folgende Leitfragen:

- **Was eignet sich für den Einstieg?**
  Nicht gleich mit komplexen Interviews starten. Besser: Ein KI-gestützter HR-Service-Desk, der Mitarbeitende bei Routinefragen unterstützt.
- **Wie sichern wir die menschliche Letztentscheidung ab?**
  Human-in-the-Loop ist Pflicht. Die KI liefert Vorschläge, aber der Mensch entscheidet – nachvollziehbar und dokumentiert. Diese Prozesse müssen klar geregelt sein – idealerweise in der Richtlinie oder per Bereichsanweisung.
- **Wie sieht ein schlanker Umsetzungsprozess aus?**
  Am Beispiel HR in drei Schritten:
  1. **Zieldefinition & Use Case-Auswahl**
     – Wozu soll die KI beitragen? Effizienz im Recruiting? Bessere Personalentwicklung? Nur sinnvolle, zielführende Anwendungen setzen sich durch.
  2. **Interdisziplinäre Risikoanalyse & rechtliche Prüfung**
     – Juristische, ethische und technische Risiken sollten frühzeitig bewertet werden, insbesondere Prüfung auf Hochrisikoeinstufung nach KI-VO, DSGVO-Konformität und Mitbestimmungsfragen.
  3. **Pilotierung & Transparenzsicherung**
     – Start mit einem messbaren, überschaubaren Projekt. Frühzeitige Einbindung aller Stakeholder (HR, Compliance, IT, Betriebsrat) ist entscheidend.

Schritt 5 – Von der Whitelist zur Richtlinie
Stehen die erlaubten Use Cases fest, ist die Grundlage für eine KI-Richtlinie geschaffen.
Was gehört in eine gute Richtlinie?

📌 Zweck, Geltungsbereich und Verantwortlichkeiten.

📌 Rechtliche Grundlagen & ethische Prinzipien – verständlich erklärt. Dazu gehören auch die Grundsätze der Nutzung, ethische Überlegungen, dass KI nur durch entsprechend geschulte Mitarbeiter eingesetzt werden darf oder dass von den definierten Einsatzzwecken nicht abgewichen werden darf, also nicht das KI-Tool ist erlaubt, sondern das KI-Tool in Kombination mit dem definierten Einsatzzweck.

📌 Globale Regeln – z. B. Verbot von sensiblen oder vertraulichen Unternehmensdaten in öffentlich zugänglichen KI-Tools oder dass die Nutzung kostenloser bzw. privater Accounts untersagt ist.

📌 Use Case-Beschreibungen – je klarer beschrieben ist, für welche Use Cases der Einsatz des KI-Tools erlaubt ist, desto besser nachvollziehbar wird dies für die Beschäftigten.

📌 Klare Bedingungen für jeden Use Case – was ist erlaubt, was ist untersagt. Wenn z.B. die Transkriptionsfunktion in Zoom genutzt werden soll muss vorher von allen Teilnehmern der Videokonferenz eine Einwilligung eingeholt werden. Wir erlauben auf der einen Seite also den Einsatz der Transkriptions-KI, stellen aber Bedingungen daran.
📌 Prozesse für neue Tools oder Use Cases – inkl. Freigabeverfahren für die Nutzung neuer KI-Systeme oder neuer Use Cases.

Hammer Home your Message
Die Richtlinie steht – wie bringen wir sie jetzt in die Köpfe der Mitarbeitenden?

Schritt 6 – Kompetenzvermittlung – doch was ist Kompetenz?
Die KI-Verordnung verlangt, dass Unternehmen Kompetenzen bei den Mitarbeitern aufbauen, die KI-Systeme einsetzen. Doch was heißt das konkret?

- Verständnis der Funktionsweise von KI-Systemen:
  Wie „denken" diese Systeme? Welche Daten verarbeiten sie? Wie entstehen die Ergebnisse?
- Bewusstsein für Chancen und Risiken:
  Wie lassen sich Potenziale heben – und gleichzeitig Fehlentscheidungen, Diskriminierung oder Sicherheitsrisiken vermeiden?
- Kenntnis der rechtlichen Rahmenbedingungen:
  Welche Pflichten gelten konkret? Und wie hängen KI-VO, DSGVO und andere Regelwerke zusammen?
- Ethische Aspekte:
  Wie gestalten wir KI-Einsatz verantwortungsvoll und wertebasiert?

Ein zentrales Instrument zur Kompetenzvermittlung ist die interne KI-Richtlinie, doch mit einer Richtlinie allein ist es nicht getan. In einer Schulung sollte man über die o.g. Themen hinaus auch die wichtigsten Regelungen der KI-Richtlinie aufgreifen und vermitteln. Doch wie erreichen wir, dass die Mitarbeiter diese nun auch umsetzen?

Schritt 7 – Aus Schulung wird gelebte Strategie
Schulungen sensibilisieren – aber sie sind nicht das Ziel, sondern der Startpunkt.
Damit aus Wissen auch Anwendung wird, müssen Unternehmen sicherstellen, dass die Regelungen der KI-Richtlinie konkret im Arbeitsalltag ankommen.
Ein zentraler Erfolgsfaktor: Integrieren Sie KI-Prozesse in bestehende Abläufe.
Beispiel:
Ihr Unternehmen hat einen etablierten Einkaufsprozess mit definierten Freigaben? Dann sollte die Beschaffung neuer KI-Systeme nicht als Sonderweg laufen, sondern Teil dieses bestehenden Procurement-Prozesses werden – inklusive Risiko- und Compliancеprüfung und interner Freigabe.
Nur durch diese Verzahnung mit den gelebten Hauptprozessen entsteht echte Wirkung – und aus Strategie wird Praxis.

Und Sie?
Sie stehen vor ähnlichen Fragen rund um die Umsetzung der KI-Verordnung?
Wir teilen gerne unsere Erfahrungen aus realen Projekten – und unterstützen Sie auf dem Weg zu einer rechtskonformen, verantwortungsvollen KI-Nutzung. Kontakt: support@v-formation.de