KI verspricht Effizienz und Tempo. Ohne Plan drohen jedoch Reibungsverluste, rechtliche Risiken und teure Korrekturen. Mit klarer Governance und pragmatischen Prozessen lässt sich das Risiko für folgenreiche Fehler verringern. Eine Checkliste.

Stolperstein 1:

Regulierung zu lange ignorieren – Die KI‑Verordnung ordnet Pflichten nach Risikoklassen. Teile gelten bereits. Spätestens bis August 2027 müssen alle Anforderungen erfüllt sein. Viele greifen schon in der Entwicklung. Nachrüstungen unter Live-Bedingungen sind teuer. Es drohen Bußgelder, Vertriebsverbote, Rückrufe, Abschaltungen und Vertrauensverluste. Wer Regulierung von Beginn an einplant, spart Zeit und Geld.

Stolperstein 2:

Kein Überblick über die eingesetzte KI und Pflichten – Ohne Inventar keine Compliance. Erst die vollständige Erfassung aller bestehenden und geplanten Use Cases – inklusive Tests – ermöglicht die Zuordnung von Rollen und Pflichten. Dokumentation ist Pflicht, nicht Kür.

Stolperstein 3:

Prozesse ohne Leitplanken – Use Cases zu sammeln, reicht nicht. Rollen und Pflichten müssen nach KI‑Verordnung festgelegt und über den gesamten Lebenszyklus überwacht werden. Ohne klare Leitlinien für Auswahl, Test, Freigabe und Dokumentation entstehen Uneinheitlichkeit, Doppelarbeit und Lücken. Nötig sind saubere Governance‑Strukturen, definierte Verantwortlichkeiten und standardisierte Prüf‑, Freigabe‑ und Überwachungsprozesse.

Stolperstein 4:

Auf Gesetze vertrauen, Verträge vergessen – Die KI‑Verordnung bleibt teils abstrakt. Lieferanten müssen nicht automatisch alle Informationen liefern, die sie zur Pflichterfüllung benötigen. Lieferumfang, Informationspflichten und Sicherheit gehören in einen Vertrag – auch wenn das Gesetz schweigt. Zudem müssen Nutzungsrechte an KI und deren Output geklärt werden.

Stolperstein 5:

Geistiges Eigentum außer Acht lassen – IP‑Risiken bestehen bei Modell, System, Input und Output. Texte, Code und Daten sind oft geschützt und ohne Erlaubnis tabu. Training mit geschützten Inhalten kann doppelt verletzen: beim Kopieren/Bearbeiten und später im Output. Verträge helfen finanziell, beseitigen aber nicht die eigene Haftung. Daher: Lizenzen prüfen, Input prüfen, Output prüfen – und alles dokumentieren.

Stolperstein 6:

KI‑Kompetenz unter‑ oder überschätzen – Ohne Grundwissen steigt das Fehlerrisiko. Anbieter und Betreiber müssen Personal schulen und ausreichende KI‑Kompetenz sichern. Wer Funktionsweise, Kennzeichnung, sichere Nutzung und Grenzen nicht kennt, bewertet Ergebnisse falsch. Ein individuelles AI‑Literacy‑Programm mit regelmäßigen Auffrischungen ist Pflicht.

Stolperstein 7:

Veränderungen und KI‑Agenten nicht einplanen – Finetuning, weiteres Training, Zweckwechsel oder Vertrieb unter eigener Marke können einzuhaltende Pflichten verändern; bei KI-Agenten kann das Ganze auch ohne menschliches Zutun passieren. Nötig sind ein strukturierter Änderungs‑Check, feste Review‑Zyklen und klare Re-Klassifizierungstrigger. Zudem gilt: Human in the Loop und ein wirksamer Kill‑Switch.

Stolperstein 8:

Compliance in der KI‑Blase – Die KI‑VO ist nicht alles. Produktbezogene Vorgaben (zum Beispiel Luftfahrt, Fahrzeuge) können vorgehen oder ergänzen. Hinzu kommen EU‑Digitalrechtsakte wie Produkthaftung, Cyber Resilience Act, Digital Services Act und Data Act. Wer den „Rest“ des Rechts ignoriert, riskiert Haftung.

Stolperstein 9:

Technologischen Wandel ignorieren – KI verändert sich laufend und kann immer mehr. Review- und Kategorisierungsprozesse müssen dies berücksichtigen und den Fortschritt antizipieren – nicht ihm hinterherlaufen.

Stolperstein 10:

Loslegen ohne Planung – „Erst mal KI, den Rest klären wir später“ ist teuer. Ohne konsistente Planung vor der Einführung von KI im Unternehmen ist die Wahrscheinlichkeit, alle Stolpersteine mitzunehmen, sehr hoch. Daher ist es ratsam, das Thema vor der Einführung des ersten Use Cases auf die Agenda zu nehmen.

Fazit: Was jetzt zu tun ist

Aus dem Vorstehenden ergeben sich ein paar „Hausaufgaben“, deren Umsetzung natürlich auf das jeweilige Unternehmen zuzuschneiden ist, um Haftungsrisiken wirksam zu begrenzen:

KI‑Verordnung auf das eigene Geschäftsmodell anwenden: Pflichten identifizieren, Compliance by Design verankern, ein Go‑Live‑Gate einführen, Minimal Viable Compliance parallel zum MVP liefern und die Roadmap bis August 2027 steuern.

Zentrales KI‑Register aufsetzen und verpflichtend nutzen: Alle Use Cases mit Rolle, Risikoklasse, Pflichten, Nachweisen und Status erfassen – vor der Beschaffung und vor dem Betrieb.

Unternehmensweite KI‑Policy und Lifecycle‑Kontrollen einführen: Auswahl, Tests, Freigaben, Dokumentation und Überwachung standardisieren; Rollen und Verantwortlichkeiten klar zuweisen.

Verträge standardisieren: Informations‑ und Mitwirkungspflichten, Audit und Sicherheit, Change‑Notices, Abnahme‑/Dokumentation, Nutzungs‑ und Output‑Rechte sowie angepasste Haftung fest verankern.

Rechte‑Clearing etablieren: Rechtekette für Modelle, Trainings‑/Eingabedaten und Outputs klären; Input‑ und Output‑Checks als Prozess‑Gates verankern.

AI‑Literacy‑Programm starten: Pflichttrainings und dokumentierte Auffrischungen einführen; Zugriffsrechte an den Schulungsstand koppeln.

Change‑Control aufsetzen: Re‑Klassifizierungs‑Trigger (Fine‑Tuning, Zweckänderung, Markenwechsel, Agenten) definieren, Human‑in‑the‑Loop und Kill‑Switch vorschreiben und regelmäßige Reviews einplanen.

Rechtslandkarte erweitern: Produktrecht, CRA, DSA, Data Act und Sektorrecht integrieren; Prozesse und Nachweise bündeln; Verantwortliche und Meilensteine benennen.

Monitoring und Re‑Tests verstetigen: Technologieradar führen, Performance/Drift/Bias messen, Nachweise aktualisieren und Verbesserungen in Standards und Modelle zurückspielen.