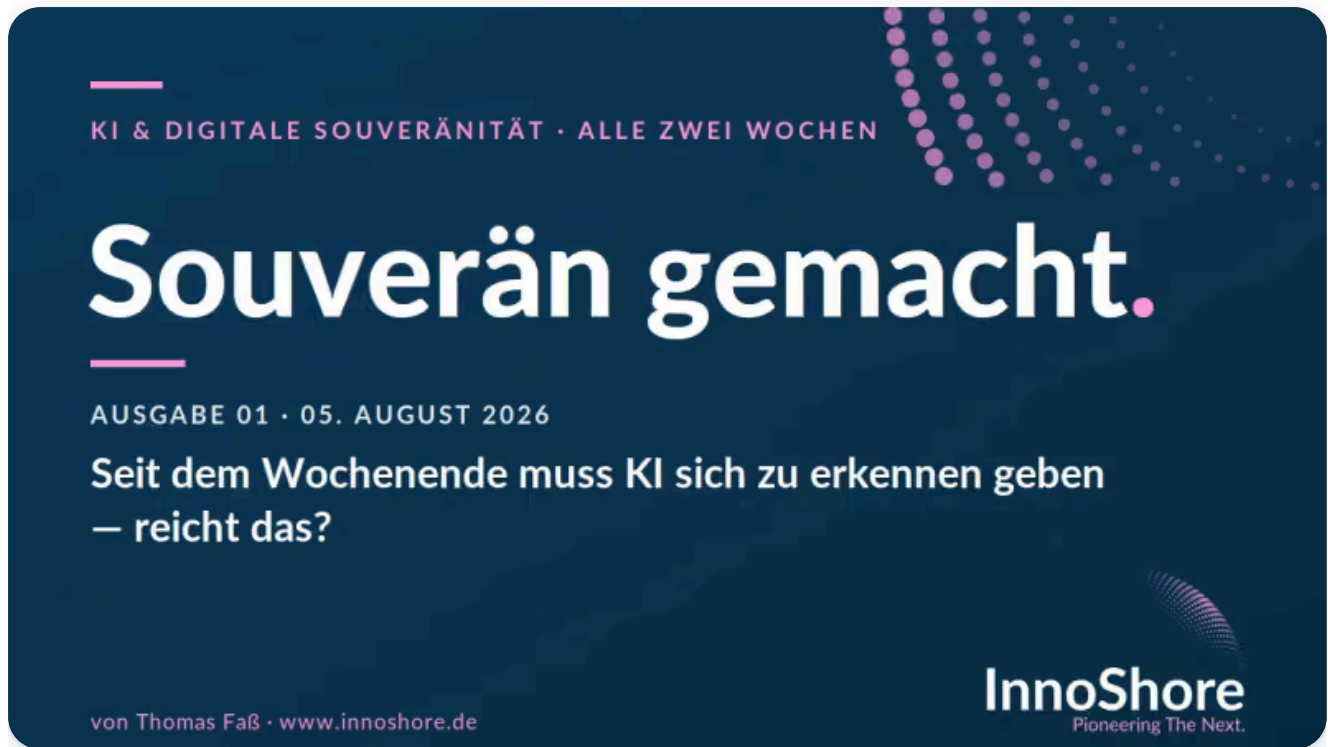


SOUVERÄN GEMACHT

Souverän gemacht #1: Seit dem Wochenende muss KI sich zu erkennen geben — reicht das?

Von Thomas Faß · 5. August 2026



Seit dem 2. August 2026 gelten die Transparenzpflichten des AI Act. Das ist ein sinnvoller Schritt — aber er beantwortet nicht die Frage, die für Ihre IT wirklich zählt: Steckt die Kontrolle über Ihre Daten in der Architektur oder nur im Vertrag?

Was seit dem 2. August gilt

Mit dem 2. August 2026 sind die Transparenzpflichten aus Artikel 50 des AI Act wirksam geworden. Sie richten sich an Anbieter und Betreiber von KI-Systemen und greifen in vier Situationen:

- Direkte Interaktion mit Menschen (Chatbots, KI-Agenten, Sprachassistenten): Nutzer müssen zu Beginn der ersten Interaktion klar erkennen können, dass sie mit einer KI sprechen.
- Synthetische Inhalte (Bild, Audio, Video, Text): KI-generierte Inhalte müssen in einem maschinenlesbaren Format als solche gekennzeichnet sein.
- Deepfakes: Bild-, Ton- oder Videomaterial, das echt wirkt, aber KI-erzeugt ist, muss offengelegt werden.
- KI-Texte zu Themen von öffentlichem Interesse: müssen gekennzeichnet werden — es sei denn, ein Mensch hat den Text redaktionell geprüft und verantwortet.

Wichtig für die Einordnung: Das ist kein pauschaler Kennzeichnungszwang. Wer KI nur unterstützend einsetzt — etwa für Rechtschreibung oder als Assistenz, ohne die Aussage wesentlich zu verändern — oder Inhalte redaktionell verantwortet, fällt nicht darunter. Privatpersonen sind ausdrücklich ausgenommen.

Zur Umsetzung hat die EU-Kommission am 20. Juli 2026 finale Leitlinien veröffentlicht und drei einheitliche Symbole bereitgestellt: „AI“, „AI generated“ und „AI modified“. Ein Detail, das in der Praxis untergeht: Das Symbol allein garantiert noch keine rechtskonforme Kennzeichnung. Und für die technische, maschinenlesbare Markierung synthetischer Inhalte durch Systeme, die bereits vor dem Stichtag auf dem Markt waren, läuft eine Nachfrist bis zum 2. Dezember 2026. Die für Nutzer sichtbaren Hinweise gelten jedoch seit dem 2. August.

Dass es die EU ernst meint, zeigt der Sanktionsrahmen: Verstöße gegen Artikel 50 können mit bis zu 15 Millionen Euro oder 3 Prozent des weltweiten Jahresumsatzes geahndet werden – je nachdem, welcher Betrag höher ist. Für kleine und mittlere Unternehmen sieht der AI Act bei der Bemessung eine besondere Berücksichtigung vor. Zeitgleich beginnt im August die Durchsetzung der Pflichten für KI-Modelle mit allgemeinem Verwendungszweck – August 2026 ist damit der erste Monat, in dem regulatorisch sowohl auf Modell- als auch auf Anwendungsebene gehandelt werden kann.

So weit die Pflicht. Interessanter ist, was sie überdeckt.

Die meisten Debatten über „souveräne KI“ drehen sich um Abschottung: eigene Cloud, eigene Modelle, Grenze zu. Das ist die falsche Fährte. Die ehrlichere Frage lautet: Wer hat die Hand am Schalter?

Souveränität wird gebaut, nicht zugesichert. Ein Anbieter, der sie über eine Auftragsverarbeitungs-Klausel und einen deutschen Serverstandort behauptet, hat sie noch nicht – der US-CLOUD-Act reicht über jeden Vertrag mit US-Muttergesellschaft, unabhängig davon, wo die Server stehen. Was zählt, steckt in der Architektur: bei welchem Modell, welchem Inferenz-Stack, welchem Datenpfad und welchem Update-Takt Sie tatsächlich bestimmen. Die Kennzeichnungspflicht erfüllen Sie mit einem Label. Die Kontrolle über Ihre Daten bekommen Sie damit nicht.

Bemerkenswert ist, dass die Debatte gerade an diesem Punkt reift. Statt Autarkie ist zunehmend von beherrschbarer Abhängigkeit die Rede – Souveränität nicht als Mauerbau, sondern als bewusst orchestrierte Partnerschaften. Das ist kein Widerspruch zu einem hybriden Liefermodell, solange das Datenführende in Deutschland und der EU bleibt und die Steuerung on-shore sitzt. Wer offenlegt, wo was läuft, darf das aufgeklebte „Sovereign“-Etikett anderer zu Recht hinterfragen.

Wie viel Souveränität braucht welcher Workload?

Wer Souveränität sauber entscheiden will, braucht ein Raster statt Bauchgefühl. Zwei Referenzen helfen dabei.

Erstens die deutsch-französische Definition digitaler Souveränität, die Deutschland und Frankreich am 17. Juni 2026 zum Auftakt der VivaTech in Paris vorgelegt haben (das „Franco-German Joint Paper on Digital Sovereignty“). Sie gliedert digitale Souveränität in sechs Dimensionen in drei Kategorien, jeweils mit Kriterienkatalogen – darunter die rechtliche Durchsetzbarkeit europäischer Regeln, der Schutz sensibler Daten und die Resilienz kritischer Infrastruktur. Sie setzt bewusst auf eigene Anbieter, Open Source und modulare Architekturen und versteht sich als freiwilliger Referenzrahmen für das EU Tech Sovereignty Package. Der praktische Wert: Die sechs Dimensionen lassen sich in Beschaffungs- und Eignungskriterien übersetzen – Souveränität wird prüfbar statt Behauptung.

Zweitens die Erkenntnis, dass Souveränität keine Ja/Nein-Frage ist, sondern eine Frage pro Workload. Nicht jeder Prozess braucht dieselbe Stufe. Maximal-Souveränität für alles ist kein Ideal, sondern Geld an der falschen Stelle. McKinsey nennt den pragmatischen Weg „minimum sufficient sovereignty“: Workloads nach ihrem regulatorischen Risiko und ihrer Abhängigkeit von Drittparteien klassifizieren und jedem die

Stufe zuweisen, die er wirklich braucht — mit expliziten Vorgaben zu Datenstandort, Schlüsselhoheit und Zugriffskontrolle. Die entscheidenden Kontrollpunkte sind souverän „by design“, der Rest bleibt offen für Partnerschaften, Interoperabilität und Wettbewerb. Das Datenführende geschützt, das Öffentliche frei.

Was das für IT-Entscheider konkret heißt

Zwischen Regulatorik und Architektur liegt ein handfester Arbeitsschritt — und der ist selten glamourös:

- Inventur. Welche KI-Vorhaben laufen bereits, offiziell oder als Schatten-IT? Welche Daten fließen jeweils hinein?
- Datenklasse bestimmen. Was ist öffentlich, was ist kundenvertraulich, was ist geschäftskritisch? Erst die Klasse entscheidet über die nötige Souveränitätsstufe — nicht der Anbieter, nicht die Schlagzeile.
- Kontrollpunkte prüfen. Wo läuft die Inferenz? Wer hält die Schlüssel? Wer kann im Ernstfall den Zugriff stoppen, ohne den halben Betrieb anzuhalten?
- Reversibilität sichern. Die unbequemste Frage zuletzt: Was können Sie mitnehmen, wenn Sie den Anbieter wechseln? Diese Fähigkeit entscheidet sich beim Aufbau — und lässt sich später nur teuer nachrüsten.

Compliance ist dabei kein Häkchen, sondern ein Nachweis. Und Innovation und Kontrolle sind kein Gegensatz — diese Zwickmühle wird Ihnen verkauft.

Fazit

Seit dem Wochenende ist Transparenz Pflicht. Aber souverän sind Sie erst, wenn Sie wissen, welcher Workload welche Stufe braucht — und wer die Hand am Schalter hat.

Diesen Newsletter schreibt Thomas Faß, Gründer von InnoShore aus Münster. InnoShore stellt Senior-IT-Experten bereit und liefert schlüsselfertige IT-Lösungen für den DACH-Mittelstand — mit Senior-Steuerung in Deutschland und einem Compliance-Baukasten, der pro Mandat konfiguriert wird, nicht von der Stange kommt.

Quellen

- [Europäische Kommission, Leitlinien zu Artikel 50 AI Act \(20.07.2026\)](#)
- [Europäische Kommission, Verhaltenskodex zu Artikel 50 AI Act \(20.07.2026\)](#)
- [Europäische Kommission, FAQ zu Artikel 50 AI Act \(20.07.2026\)](#)
- [BMDS / heise online zur deutsch-französischen Souveränitäts-Definition \(VivaTech, 17.06.2026\)](#)
- [McKinsey, „Sovereign AI ecosystems“ \(2026\)](#)
- [TÜV Rheinland zum Sanktionsrahmen \(Art. 99\).](#)

SOUVERÄN GEMACHT

Den Newsletter abonnieren

Lesen Sie jede Ausgabe zu KI-Governance und digitaler Souveränität direkt in Ihrem Feed – über unseren LinkedIn-Newsletter „Souverän gemacht“.

[Newsletter auf LinkedIn abonnieren](#)

Die Anmeldung zum Newsletter direkt hier auf der Seite steht in Kürze zur Verfügung.