KI-Allianz

KI-PROJEKTBÜRO

Monatlicher KI-Hintergrund-Newsletter

KI-Allianz Rheinland-Pfalz

KI-Allianz Rheinland-Pfalz - Monatlicher KI-Hintergrund-Newsletter

August 2026

EU AI Act & DSGVO für KMU: Was jetzt gilt - und was als Nächstes kommt

Was gilt jetzt - und was kommt als Nächstes?

Viele KMU fragen sich: Wenn wir KI nutzen, was müssen wir jetzt konkret tun - und was kann warten? Diese Ausgabe bündelt die bereits aktiven Pflichten, die wichtigsten kommenden Termine und ihre Bedeutung für typische KI-Anwendungen in KMU.

Warum das jetzt wichtig ist

Nicht jeder KI-Anwendungsfall wird gleich behandelt. Einige Pflichten gelten bereits im Alltag, besonders bei personenbezogenen Daten. Andere werden später relevant, vor allem bei Hochrisiko-KI. Ein einfaches Inventar und klare Regeln helfen, vorbereitet zu sein, ohne jedes Experiment zu einem Rechtsprojekt zu machen.

Die wichtigsten Daten auf einen Blick

25. MAI 2018	DSGVO: personenbezogene Daten Zweck und Rechtsgrundlage; Daten minimieren; informieren; Rechte; Aufbewahrung/Sicherheit; Anbieter- und Auftragsverarbeiterprüfung; DSFA und Art. 22-Schutzmaßnahmen, sofern erforderlich.
2. FEB. 2025	KI-Kompetenz und verbotene Praktiken Verhältnismäßige KI-Kompetenzmaßnahmen. Verbotene Beispiele sind schädliche Manipulation, Social Scoring, Gesichtsbilder-Scraping, bestimmte biometrische Nutzungen und meist Emotionserkennung am Arbeitsplatz.
2. AUG. 2026	Art. 50-Transparenz und Durchsetzung Wo ausgelöst: KI-Interaktion offenlegen und Deepfakes oder bestimmte KI-generierte Inhalte von öffentlichem Interesse kennzeichnen. Durchsetzung anwendbarer Pflichten läuft.
2. DEZ. 2026	Zusätzliche Verbote und Übergang Neue Verbote für KI-generierte/manipulierte nicht-einvernehmliche intime Inhalte und Material sexualisierten Kindesmissbrauchs; ein begrenzter Art.-50-Übergang endet.
2. DEZ. 2027	Annex-III-Hochrisiko-KI-Pflichten Beispiele: Recruiting, Beschäftigte, Bildung, Kredit, Lebens- oder Krankenversicherung, bestimmte Biometrie und kritische Infrastruktur.
2. AUG. 2028	Hochrisiko-KI in regulierten Produkten KI als reguliertes Produkt oder Sicherheitskomponente; Schnittstelle zu Produkt-Compliance.

Vereinfachte Orientierung - keine Rechtsberatung. Ob eine Pflicht gilt, hängt von der konkreten Rolle und vom jeweiligen Anwendungsfall ab.

Was die aktuellen Pflichten in der Praxis bedeuten

DSGVO - immer wenn personenbezogene Daten beteiligt sind

Personenbezogene Daten können in Prompts, hochgeladenen Dateien, Logs, Ausgaben oder KI-gestützten Entscheidungen auftauchen. KMU sollten Zweck und Rechtsgrundlage festlegen, Daten minimieren, erforderliche Informationen bereitstellen, Betroffenenrechte ermöglichen und Regeln zu Aufbewahrung und Sicherheit definieren.

Zu prüfen sind Auftragsverarbeitung, Unterauftragsverarbeiter, internationale Übermittlungen, Speicherfristen und Modelltraining. Eine DSFA ist vor Verarbeitungen erforderlich, die voraussichtlich ein hohes Risiko erzeugen; Schutzmaßnahmen gelten bei ausschließlich automatisierten Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung.

KI-Kompetenz und verbotene Praktiken - bereits aktiv

Artikel 4 verlangt verhältnismäßige Maßnahmen zur KI-Kompetenz von Beschäftigten und anderen Personen, die im Auftrag der Organisation KI nutzen oder betreiben. Es gibt keinen vorgeschriebenen Kurs, keine Prüfung und kein Zertifikat. Praktisch ist ein kurzer Grundbaustein für alle plus rollenbezogene Hinweise für HR, Marketing, IT, Einkauf und Führungskräfte.

Verbotene Beispiele sind schädliche Manipulation oder Ausnutzung, Social Scoring, ungezieltes Scraping von Gesichtsbildern, bestimmte sensible biometrische Kategorisierung und Emotionserkennung am Arbeitsplatz außer in engen medizinischen oder sicherheitsbezogenen Situationen.

Transparenzpflichten - wo sie ausgelöst werden

Relevante Pflichten umfassen: Menschen über KI-Interaktion informieren; Personen über Emotionserkennung oder biometrische Kategorisierung informieren; Deepfakes und bestimmte KI-generierte Texte von öffentlichem Interesse klar kennzeichnen. Maschinenlesbare Kennzeichnungen betreffen vor allem Anbieter.

Anbieter-Hinweis

Nicht automatisch annehmen: "Wir nutzen doch nur ein Anbieter-Tool." Wenn ein KMU ein KI-System unter eigenem Namen anbietet, es wesentlich verändert oder den Zweck ändert, können Anbieterpflichten auf das KMU übergehen. Das sollte fachlich geprüft werden.

Hochrisiko-KI: vorbereiten, nicht in Panik verfallen

Annex-III-Hochrisiko-KI - ab 2. Dezember 2027

Für KMU relevante Beispiele können Recruiting und CV-Filterung, Beschäftigtenmanagement oder -überwachung, Bildungsbewertung, Kreditwürdigkeitsprüfung, Lebens- oder Krankenversicherung, bestimmte biometrische Nutzungen und kritische Infrastruktur sein. Betreiberpflichten umfassen u. a. Gebrauchsanweisungen, kompetente menschliche Aufsicht, Kontrolle relevanter Eingabedaten, Monitoring, Aussetzen und Melden schwerer Risiken oder Vorfälle, Log-Aufbewahrung und Information von Beschäftigten vor dem Einsatz am Arbeitsplatz.

Hochrisiko-KI in regulierten Produkten - ab 2. August 2028

Dies gilt, wenn KI ein reguliertes Produkt oder eine Sicherheitskomponente ist. Für viele KMU bleibt dies ein Spezialfall, wird aber in Produktumfeldern wie Maschinen oder Medizinprodukten wichtig und muss mit Produkt-Compliance koordiniert werden.

60-Sekunden-Triage je KI-Anwendungsfall

1. Rolle: Nur Betreiber - oder führen eigenes Branding, wesentliche Veränderung oder geänderter Zweck zum Anbieterstatus?
2. Personenbezogene Daten: Identifizieren Prompts, Dateien, Logs, Ausgaben oder Entscheidungen Menschen?
3. Verbotene Praktiken: Geht es um verbotene Manipulation, Social Scoring, Emotionserkennung am Arbeitsplatz oder verbotene biometrische Nutzung?
4. Transparenz: Ist die KI öffentlich sichtbar, oder erstellt/nutzt sie synthetische Inhalte, Deepfakes, Emotionserkennung oder biometrische Kategorisierung?
5. Hochrisiko-Auslöser: Betrifft der Fall Recruiting, Beschäftigte, Bildung, Kredit, Lebens- oder Krankenversicherung, Biometrie, kritische Infrastruktur oder ein reguliertes Produkt?

Was KMU jetzt tun sollten

1. Ein einfaches KI-Inventar anlegen: Tool, Anbieter, Zweck, Verantwortliche, Nutzende, betroffene Personen, beteiligte Daten und aktueller Status.
2. Grundlegende KI-Kompetenz für alle Nutzenden schaffen und kurze rollenbezogene Hinweise für HR, Marketing, IT, Einkauf und Management bereitstellen.
3. Regeln zu freigegebenen Tools und menschlicher Prüfung festlegen: Welche Daten dürfen eingegeben werden, was darf nicht eingegeben werden, und welche Ausgaben müssen immer verifiziert oder freigegeben werden?
4. Anbieter und Vertrag prüfen: Sicherheit, Speicherfristen, Nutzung für Modelltraining, Unterauftragsverarbeiter, Übermittlungen und Auftragsverarbeitungsbedingungen.
5. Schlanke Nachweise aufbewahren: Unterweisungen, Verantwortliche, Prüfzeitpunkte, Vorfälle, Zweckänderungen und nächsten Review-Termin.

Ausblick

Es geht nicht darum, aus jedem KMU eine Compliance-Abteilung zu machen. Es geht darum, KI-Nutzung strukturierter, sicherer und zukunftsfester zu gestalten. Ein Inventar, grundlegende KI-Kompetenz, klare Tool-Regeln und frühe Aufmerksamkeit für sensible oder potenziell hochriskante Anwendungsfälle schaffen bereits eine starke Grundlage.

Inhalte zusammengestellt vom KI-Projektbüro der KI-Allianz Rheinland-Pfalz,
unterstützt durch den Lehrstuhl Maschinelles Lernen an der RPTU in Kaiserslautern.
Steffen Reithermann <steffen.reithermann@cs.rptu.de> - ml.cs.rptu.de
Newsletter-Archiv: https://ml.cs.rptu.de/projects/KI-Projektbuero/newsletter/
Virtuelle Plattform der KI-Allianz Rheinland-Pfalz: https://www.ki-allianz-rlp.de/
Website des KI-Projektbüros: https://ml.cs.rptu.de/projects/KI-Projektbuero/

RPTU

Rheinland-Pfälzische
Technische Universität
Kaiserslautern
Landau