Luther.

KI-Omnibus 2026: Was Unternehmen jetzt wissen müssen



Mit der finalen Zustimmung des Rates der Europäischen Union vom 29. Juni 2026 ist das Gesetzgebungsverfahren für die Digital-Omnibus-Verordnung zur KI abgeschlossen. Der KI-Omnibus passt die bereits in Kraft getretene KI-Verordnung punktuell an: Insbesondere werden einzelne Fristen verschoben, zentrale Begriffe präzisiert und Erleichterungen für bestimmte Unternehmenskategorien geschaffen. Für Unternehmen bedeutet das: mehr Zeit, aber keine Entwarnung. Wer KI entwickelt, vertreibt, integriert oder nutzt, sollte jetzt prüfen, welche Systeme betroffen sind, welche Pflichten erfüllt werden müssen und wo weiterhin Handlungsbedarf besteht. Die nachfolgenden Ausführungen bieten einen kompakten Überblick über die zentralen Änderungen der KI-VO einschließlich des neuen Zeitplans für den Geltungsbeginn der einzelnen Vorschriften.

I. Die wichtigsten Änderungen im Überblick

Verschiebung des Anwendungsbeginns

- Festlegung neuer Stichtage für Geltungsbeginn eines Großteils der Vorgaben für Hochrisiko-KI
- Schaffung eines neuen Übergangszeitraums für den Geltungsbeginn der Pflichten aus Art. 50 KI-VO

Erleichterungen für kleine Midcap-Unternehmen

- Betrifft insbesondere die Erstellung der technischen Dokumentation und die Einrichtung eines Qualitätsmanagementsystems für Hochrisiko-KI

Abschwächung der KI-Kompetenz

- Die Pflicht zur Sicherstellung eines ausreichenden Maßes an KI-Kompetenz des Personals gem. Art. 4 KI-VO wird deutlich abgeschwächt

Rechtsgrundlage für die Verarbeitung personenbezogener Daten

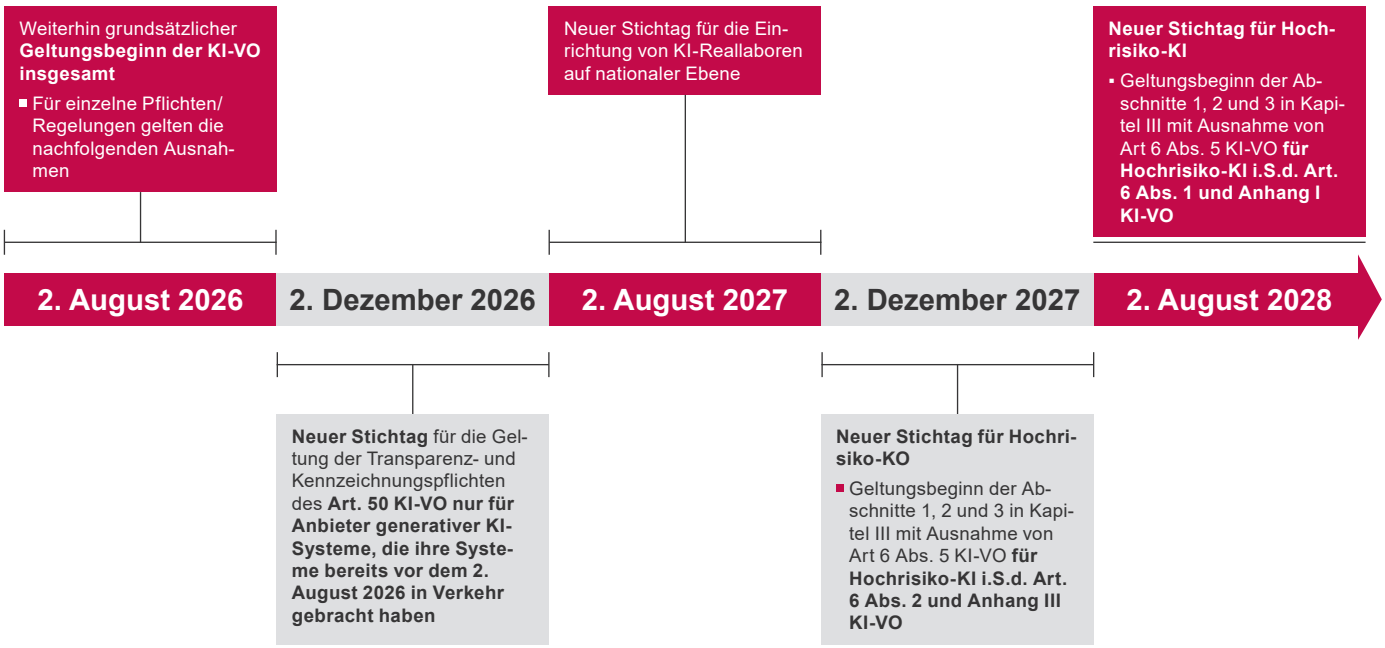
- Erweiterung der bereits bestehenden Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten unter bestimmten Voraussetzungen

Erweiterung der verbotenen Praktiken

- Ergänzung von verbotenen Praktiken im Katalog des Art. 5 KI-VO Betrifft KI-generiertes Missbrauchsmaterial

unyer GLOBAL ADVISORS

II. Compliance-Fahrplan: Die Stichtage der KI-VO bis 2028



III. Zentrale Änderungen im Detail

Bisherige Definition des Sicherheitsbauteils in der KI-VO:	**Eingrenzung des Begriffs des Sicherheitsbauteils im KI-Omnibus 2026**
Praktische Relevanz: Der Begriff des Sicherheitsbauteils entscheidet mit darüber, ob ein KI-System als Hochrisiko-KI-System einzustufen ist. Je enger der Begriff gefasst wird, desto eher können KI-Systeme aus dem strengen Hochrisiko-Regime herausfallen.	
▪ Gem. Art. 3 Nr. 14 KI-VO ist ein Sicherheitsbauteil ein Bestandteil eines Produkts oder KI Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet ▪ Nach bisherigem Art. 6 Abs. 1 KI-VO gilt ein KI-System als Hochrisiko-KI-System, wenn es selbst ein reguliertes Produkt nach Anhang I KI-VO ist oder als Sicherheitsbauteil eines solchen Produkts verwendet werden soll. Zusätzlich muss das Produkt oder das KI-System selbst vor dem Inverkehrbringen oder der Inbetriebnahme einer Konformitätsbewertung durch Dritte unterliegen.	▪ Gem. **Art. 3 Nr. 14 KI-VO** ist ein Sicherheitsbauteil ein Bestandteil eines Produkts oder KI-Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet; für die Zwecke dieser Begriffsbestimmung erfüllt ein Bauteil dann eine Sicherheitsfunktion, wenn seine Zweckbestimmung darin besteht, Risiken für die Gesundheit und Sicherheit von Personen oder Eigentum abzuwenden oder zu mindern. ▪ Art. **6 Abs. 1 lit. a-c KI-VO** stellt darüber nunmehr klar: Ein KI-System ist nicht automatisch ein Sicherheitsbauteil, nur weil es in ein reguliertes Produkt integriert ist. Maßgeblich ist, ob dessen Ausfall oder Fehlfunktion Gesundheit oder Sicherheit gefährden würde. Reine Funktionen zur Nutzerunterstützung, Leistungsoptimierung, Effizienzsteigerung, Automatisierung, Benutzerfreundlichkeit oder Qualitätskontrolle ohne Sicherheitsbezug gelten nicht als Sicherheitsbauteil.

Anforderungen an die KI-Kompetenz in der KI-VO bisher:	Beschränkung der Anforderungen an die KI-Kompetenz
▪ Gem. Art. 4 KI-VO ergreifen die Anbieter und Betreiber von KI-Systemen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI Systemen befasst sind, über ein ausreichendes Maß an KI Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI Systeme eingesetzt werden sollen, zu berücksichtigen sind.	▪ In dem neuen Art. 4 Abs. 1 KI-VO findet sich nunmehr die Ergänzung, dass diese Verpflichtung zur Unterstützung der KI-Kompetenz des Personals Anbieter und Betreiber nicht dazu verpflichtet, für irgendeine Person ein bestimmtes Niveau an KI-Kompetenz zu garantieren. ▪ Die Vorgabe verschwindet damit nicht, wird aber entschärft: Statt einer strikt verpflichtenden und sanktionierten Regelung steht künftig stärker ein unterstützender Umsetzungsansatz im Vordergrund.
Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten bisher:	**Erweiterung der Rechtsgrundlage im KI-Omnibus 2026**
▪ Bislang gab es in Art. 10 Abs. 5 KI-VO nur für Anbieter von Hochrisiko-KI-Systemen eine Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten zum Zwecke der Erkennung und Korrektur von Verzerrungen.	▪ Diese Rechtsgrundlage wird mit dem KI-Omnibus aus Art. 10 Abs. 5 KI-VO herausgelöst und in einen eigenständigen Art. 4a KI-VO überführt. ▪ Soweit die in Art. 4a KI-VO aufgeführten Bedingungen erfüllt sind, können sich nicht nur Anbieter von Hochrisiko-KI-Systemen auf die Rechtsgrundlage stützen, sondern auch deren Betreiber sowie Anbieter und Betreiber anderer KI-Systeme und -Modelle. ▪ Die Rechtsgrundlage unterliegt aber nach wie vor denselben Begrenzungen, Bedingungen und Schutzmaßnahmen wie bisher.

IV. Entlastungen für kleine Midcap-Unternehmen

Der KI-Omnibus erweitert bestimmte Erleichterungen, die bislang vor allem KMU und Start-up-Unternehmen zugutekamen, auf kleine Midcap-Unternehmen. Darunter fallen nach der Definition des neuen Art. 3 Nr. 14b KI-VO i.V.m. Nr. 2 des Anhangs der Empfehlung (EU) 2025/1099 Unternehmen, die keine KMU sind, aber weniger als 750 Personen beschäftigen und einen Jahresumsatz von höchstens 150 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 129 Mio. EUR beläuft. Praktisch relevant ist dies vor allem für Anbieter von Hochrisiko-KI-Systemen: Sie können insbesondere bei der Bereitstellung der technischen Dokumentation und der Einrichtung eines Qualitätsmanagementsystems von vereinfachten Anforderungen profitieren. Zudem sollen KMU und kleine Midcap-Unternehmen einen bevorzugten Zugang zu den auf nationaler Ebene sowie auf Unionsebene zu errichtenden KI-Reallaboren erhalten. Für wachstumsstarke Unternehmen lohnt sich daher eine Prüfung, ob sie künftig unter diese neue Kategorie fallen und dadurch Compliance-Aufwand reduzieren können.

V. Datenschutz und Bias-Kontrolle

Der KI-Omnibus erweitert die Möglichkeit, besondere Kategorien personenbezogener Daten zur Erkennung und Korrektur von Verzerrungen in KI-Systemen zu verarbeiten. Diese

Befugnis wird aus dem Kapitel in der KI-VO zu Hochrisiko-Systemen herausgelöst und kann künftig auch für Betreiber sowie für andere KI-Systeme und KI-Modelle relevant werden. Eine pauschale Lockerung der datenschutzrechtlichen Anforderungen an die Verarbeitung besonderer Kategorien personenbezogener Daten ist damit aber nicht verbunden: Die Verarbeitung bleibt nur ausnahmsweise zulässig, wenn sie unbedingt erforderlich ist und der Zweck nicht mit anonymisierten, synthetischen oder sonst weniger sensiblen Daten erreicht werden kann. Unternehmen sollten deshalb vorab dokumentieren, warum sensible Daten benötigt werden, welche Schutzmaßnahmen greifen und wann die Daten wieder gelöscht werden.

VI. Erweiterung des Katalogs der verbotenen Praktiken in Art. 5 KI-VO

Der KI-Omnibus erweitert den Katalog der verbotenen KI-Praktiken in Art. 5 KI-VO um besonders missbrauchsanfällige generative KI-Anwendungen. Künftig untersagt sind KI-Systeme, mit denen realistisch wirkende intime oder sexuelle Inhalte über bestimmbare natürliche Personen ohne deren ausdrückliche Zustimmung erzeugt oder manipuliert werden können. Ebenfalls verboten werden KI-Systeme, die Darstellungen sexuellen Kindesmissbrauchs (sog. CSAM) erzeugen oder manipulieren. Die Verbote betreffen sowohl Anbieter, die solche KI-Systeme auf dem Unionsmarkt bereitstellen, als auch Betreiber, die entsprechende Systeme zu den aufgeführten Zwecken einsetzen.

VII. Fazit und Handlungsempfehlungen

Der KI-Omnibus bringt vor allem punktuelle Entlastungen, Klarstellungen und Fristverschiebungen – aber keine generelle Verschiebung des Geltungsbeginns sämtlicher Vorschriften der KI-VO. Für Unternehmen kommt es deshalb jetzt darauf an, die Änderungen gezielt auszuwerten und nicht pauschal davon auszugehen, dass KI-Compliance insgesamt später relevant wird.

Es empfiehlt sich daher folgendes Vorgehen:

- Fristen konkret prüfen: Welche Pflichten werden tatsächlich verschoben, welche gelten weiter?
- Sicherheitsbauteile neu bewerten: Bei produktintegrierter KI prüfen und dokumentieren, ob ein echter Sicherheitsbezug besteht.
- Bias-Daten absichern: Personenbezogene Daten besonderer Kategorien zu diesem Zweck weiterhin nur bei strenger Erforderlichkeit und mit klaren Schutz- und Löschkonzepten verarbeiten.
- Midcap-Erleichterungen nutzen: Prüfen, ob die Schwellenwerte für Midcap-Unternehmen eingehalten werden und ob ggf. vereinfachte Dokumentations- und Qualitätsmanagementanforderungen genutzt werden können.
- Generative KI absichern: Neue Verbote in Art. 5 KI-VO durch technische Sperren, Moderation und klare Nutzungsregeln praktisch umsetzen.

Ihre Ansprechpartner



Dr. Michael Rath
Rechtsanwalt, Certified Information Privacy Professional/Europe (CIPP/E), Fachanwalt für IT-Recht, Partner
Köln
T +49 221 9937 25795
michael.rath@luther-lawfirm.com



Christian Kuß, LL.M.
Rechtsanwalt, Partner
Köln
T +49 221 9937 25686
christian.kuss@luther-lawfirm.com