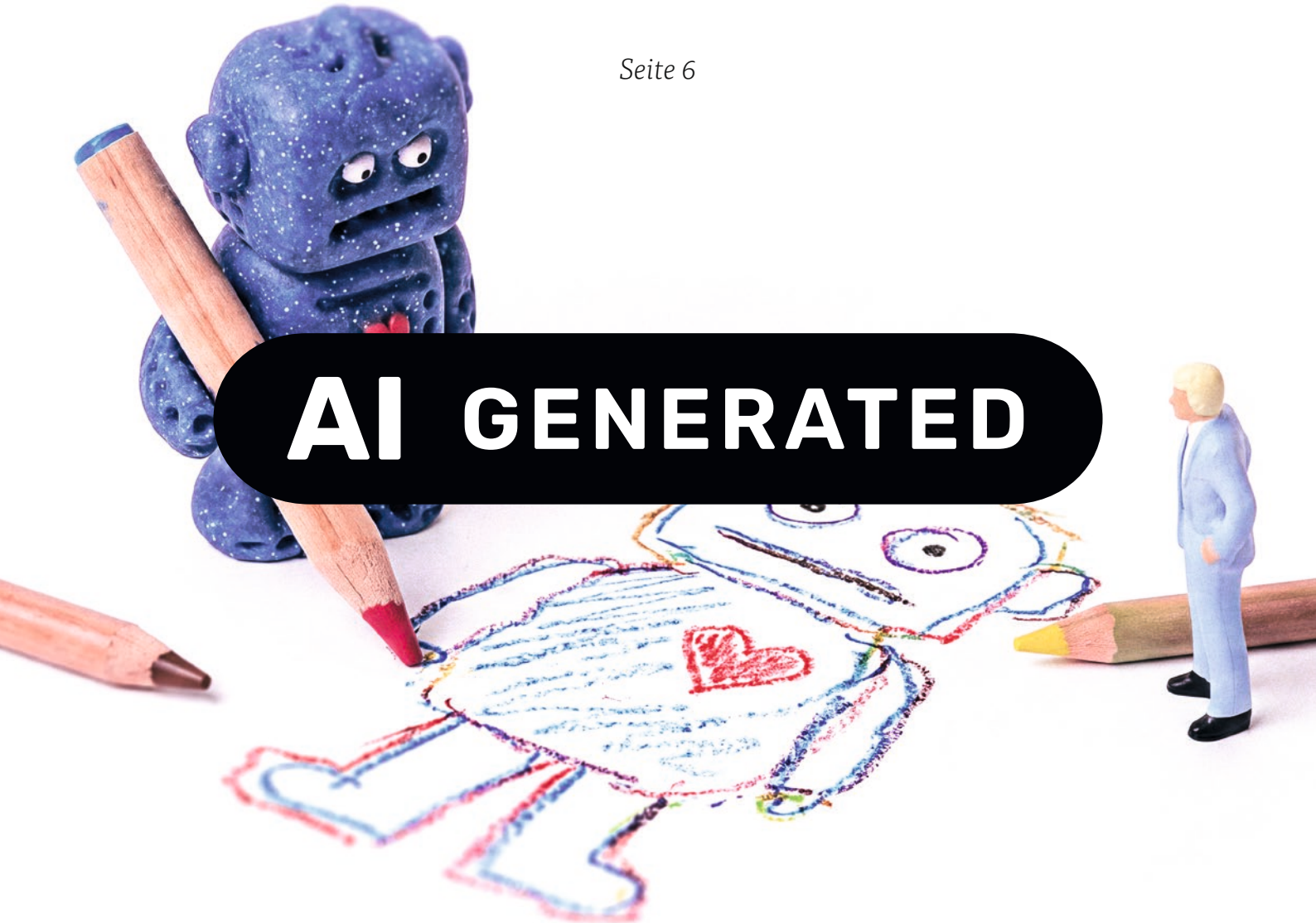
COMPLIANCE konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 3/2026

KI-Kennzeichnung

Seit dem 2. August müssen KI-generierte Inhalte klar erkennbar gemacht werden. Was bedeutet das konkret?

Seite 6



Editorial

Liebe Leserin, lieber Leser,

die Digitalisierung entwickelt sich mit hoher Geschwindigkeit weiter. Neue Technologien eröffnen Chancen für effizientere Prozesse, bessere Zusammenarbeit und innovative Dienstleistungen. Gleichzeitig verändern sich die regulatorischen Anforderungen kontinuierlich. Für Unternehmen und Organisationen wird es daher immer wichtiger, technologische Entwicklungen nicht isoliert zu betrachten, sondern sie sicher, rechtskonform und strategisch einzuordnen.

Im Mittelpunkt dieser Ausgabe steht die neue KI-Kennzeichnungspflicht. Sie verpflichtet Unternehmen, KI-generierte Inhalte und den Einsatz von KI-Systemen transparent zu machen. In unserem Leitartikel zeigen wir, worauf Sie jetzt achten müssen und wie Sie die Anforderungen praktisch umsetzen. Darüber hinaus beleuchten wir weitere Themen, die viele Verantwortliche bereits heute beschäftigen. Wir werfen einen Blick auf Startups und die Frage, wie Datenschutz von Beginn an sinnvoll mitwachsen kann, statt später zum kostspieligen Hindernis zu werden.

Auch im Bereich der KI-Governance bleibt die Dynamik hoch. Die neuen EU-Leitlinien zur Risikoeinstufung von KI-Systemen sorgen für mehr Orientierung bei der praktischen Umsetzung der KI-Verordnung. Sie helfen Unternehmen dabei, Risiken besser einzuordnen und die richtigen Maßnahmen abzuleiten. Ergänzend beleuchten wir den Cyber Resilience Act, mit dem der europäische Gesetzgeber seine Anforderungen an den Schutz digitaler Produkte konkretisiert.

Allen Beiträgen dieser Ausgabe ist eines gemeinsam: Compliance ist längst kein Selbstzweck mehr. Datenschutz, Informationssicherheit und KI-Governance schaffen Vertrauen, reduzieren Risiken und bilden die Grundlage für eine zukunftsfähige Digitalisierung. Wer frühzeitig klare Strukturen schafft und regulatorische Entwicklungen als Chance versteht, gewinnt Handlungsspielräume statt zusätzlicher Bürokratie.

In eigener Sache möchte ich Ihnen noch eine persönliche Nachricht mitteilen: Meinen Mitgründer und langjährigen Partner Niels Kill haben wir vor Kurzem in den Ruhestand verabschiedet. Wir wünschen ihm für die kommende Zeit alles erdenklich Gute.

Ich wünsche Ihnen eine informative Lektüre und viele praxisnahe Impulse für Ihre tägliche Arbeit.

Herzliche Grüße

Thomas Althammer

Darüber wird gesprochen

KLICK/SCAN

Weitere aktuelle Themen sowie die Anmeldemöglichkeit für den Althammer & Kill-Newsletter finden Sie unter: *althammer-kill.de/news*

In eigener Sache: Zeit für Veränderungen

Nach vielen gemeinsamen und ereignisreichen Jahren ist für mich die Zeit gekommen, mich von Althammer & Kill zu verabschieden.

Natürlich gehe ich mit einem weinenden und einem lachenden Auge. Althammer & Kill aufzubauen, weiterzuentwickeln und gemeinsam mit vielen großartigen Menschen wachsen zu sehen, war für mich eine besondere Zeit, auf die ich mit Stolz zurückblicke. Gleichzeitig freue ich mich auf das, was vor mir liegt. Und ich bin mir sicher, dass auch für Althammer & Kill viele weitere erfolgreiche Jahre bevorstehen. Ich möchte mich bei allen Kolleginnen und Kollegen, Kunden und Wegbegleitern für das Vertrauen, die Zusammenarbeit und die vielen Begegnungen bedanken.

Alles Gute und auf ein Wiedersehen!
Ihr Niels Kill

NIS-2: Vom Gesetz in die Praxis

NIS-2 ist in Deutschland geltendes Recht – für betroffene Unternehmen und Organisationen geht es jetzt um die konkrete Umsetzung. Doch welche Anforderungen gelten und wo besteht noch Handlungsbedarf?

Unser aktualisiertes NIS-2-Whitepaper mit Quick-Check bietet Orientierung: Es zeigt kompakt, wer betroffen ist, welche Pflichten zu beachten sind und welche Schritte jetzt wichtig sind. Der integrierte Quick-Check hilft dabei, die eigene Situation besser einzuschätzen und erste Handlungsfelder zu identifizieren. Das Whitepaper „NIS-2 Handlungsbedarf für Unternehmen und Organisationen" ist ab sofort auf unserer Homepage zum kostenlosen Download abrufbar. Jetzt einfach runterladen!

KLICK/SCAN

Innovationspotenziale von Künstlicher Intelligenz in Stadtplanung, -entwicklung und -verwaltung

Künstliche Intelligenz kann Kommunen dabei unterstützen, Stadtentwicklung, Mobilität und Bürgerservices effizienter zu gestalten. Der größte Hebel liegt jedoch nicht in der Technologie selbst, sondern in einer klaren Governance, einer guten Datenbasis und einer frühzeitigen Einbindung von Datenschutz und Compliance. So gelingt der Weg von der Pilotphase in den produktiven Einsatz.

KLICK/SCAN

Phishing und Social Engineering in 2026: Warum Vertrauen kein Sicherheitskonzept ist

Phishing-Angriffe werden durch KI immer professioneller und sind oft kaum noch zu erkennen. Unternehmen sollten deshalb nicht allein auf die Aufmerksamkeit ihrer Mitarbeitenden setzen. Entscheidend sind klare Sicherheitsprozesse, phishingresistente Authentifizierung und eine gelebte Meldekultur, um Angriffe frühzeitig zu erkennen und Schäden zu begrenzen.

KLICK/SCAN

Datenübermittlungen in die USA und der „Untergang des Abendlandes"?

Die Entscheidung des US Supreme Court im Fall Trump v. Slaughter sorgt für Diskussionen über die Zukunft des EU-US Data Privacy Frameworks. Der Angemessenheitsbeschluss gilt jedoch weiterhin. Unternehmen sollten die Entwicklung aufmerksam verfolgen, ihre Datenübermittlungen dokumentieren und Transfer Impact Assessments sowie Standardvertragsklauseln überprüfen – akuter Handlungsbedarf besteht derzeit jedoch nicht.

KLICK/SCAN

Meetings aufzeichnen und transkribieren: Datenschutz beginnt vor dem Klick auf „Starten"

Online-Meetings sind heute Arbeitsort, Entscheidungsplattform und Schulungsraum in einem. Automatische Transkription klingt da nach naheliegender Effizienzmaßnahme: keine Mitschrift, schnellere Protokolle, nachvollziehbare Entscheidungen. Rechtlich ist das jedoch kein Komfortfeature. Sprache, Bild, Chat und Metadaten sind personenbezogene Daten. In nicht öffentlichen Meetings greift zusätzlich § 201 StGB. Wer Transkription einführt, braucht einen klaren rechtlichen und organisatorischen Rahmen.

KLICK/SCAN

Zahl des Monats

13 %

der Unternehmen berichten bereits von Sicherheitsvorfällen im Zusammenhang mit KI-Anwendungen oder KI-Modellen. Gleichzeitig gaben 97 % der betroffenen Organisationen an, dass angemessene Zugriffs- und Sicherheitskontrollen für KI fehlten. KI-Governance entwickelt sich damit zunehmend vom Zukunftsthema zur konkreten Managementaufgabe.

Akademie

KLICK/SCAN

Mehr Infos und Anmeldung unter: *althammer-kill.de/akademie*

2. Oktober // 7. Oktober 2026 – Online-Seminar

NIS-2 Management Pflichtschulung

Diese Schulung richtet sich gezielt an Geschäftsleitungen und Führungskräfte und vermittelt praxisnah, wie Sie Ihre Organisation wirksam und gesetzeskonform aufstellen. Mit Abschluss dieser Schulung leisten Sie zugleich einen wichtigen Beitrag zur Erfüllung Ihrer Pflichten gemäß des im NIS-2-Umsetzungsgesetz geänderten § 38 BSIG – insbesondere im Hinblick auf die Qualifizierung der Geschäftsleitung in Fragen der Cybersicherheit.

27.–28. Oktober 2026 – Online-Seminar

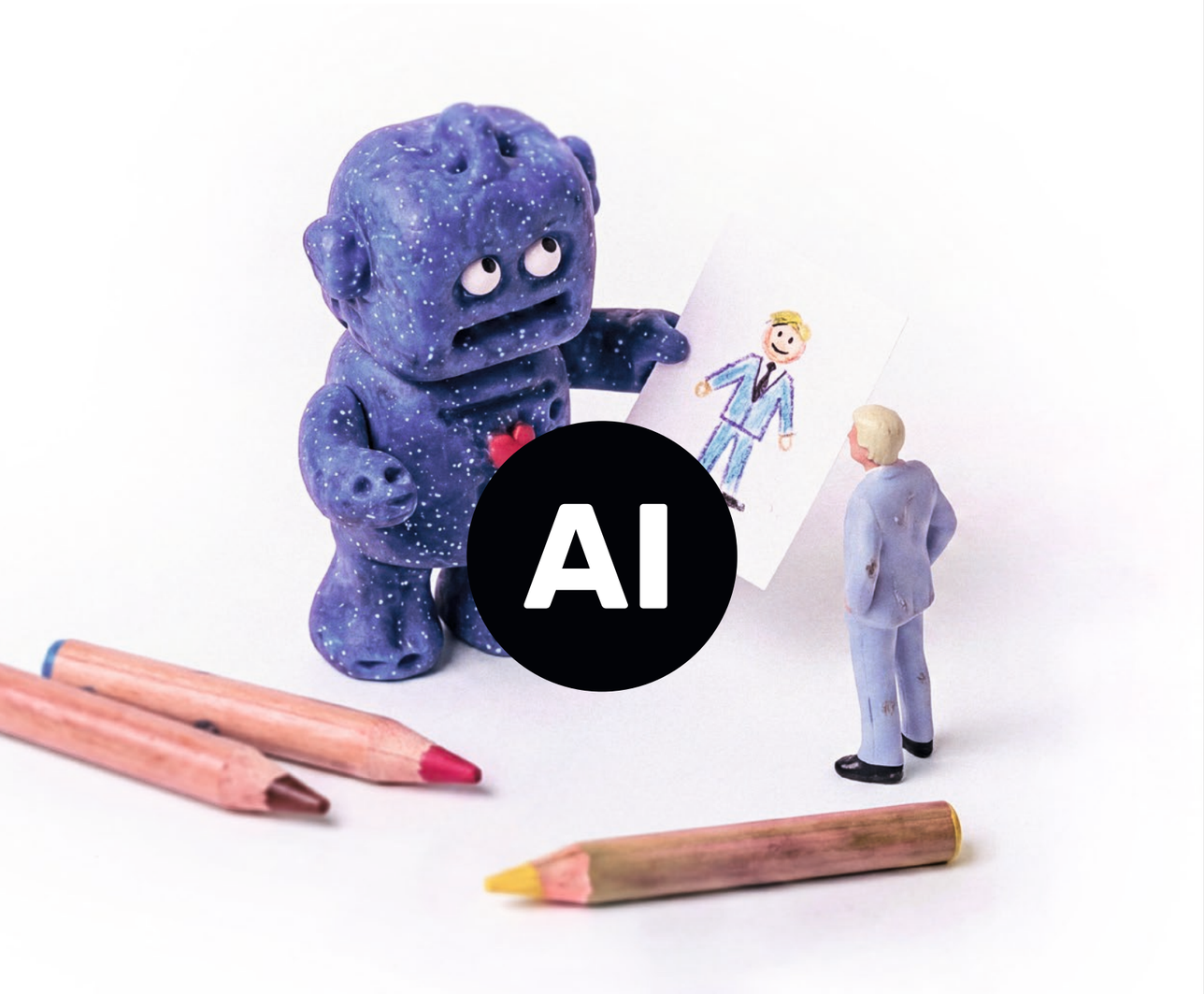
Datenschutzkoordinator/in DSGVO, DSG-EKD & KDG

Auch wenn keine Datenschutzbeauftragten bestellt werden müssen, sind Datenschutzgesetze und -regelungen einzuhalten und umzusetzen. Hier kommt der Datenschutzkoordinator bzw. die Datenschutzkoordinatorin als fachliche Unterstützung der Unternehmensleitung und Mitarbeitenden ins Spiel. Sie haben einen internen oder externen Datenschutzbeauftragten? Mit dem Lehrgang Datenschutzkoordinator/in erwerben Sie das notwendige Grundlagenwissen, um Datenschutzbeauftragte bei deren Arbeit fachgerecht zu unterstützen und kompetenter Ansprechpartner zu sein.

17.–18. Februar 2027, Hannover

Das Norddeutsche KI-Forum 2027

Der 360°-Blick auf KI in Unternehmen und Behörden. Zwei Tage Keynotes, Workshops, echte Use Cases und Ausstellung – für Entscheiderinnen und Entscheider aus Verwaltung, Kommunen und Mittelstand in Norddeutschland. Jetzt Frühbucher-Tickets sichern!



KI-Kennzeichnung

Unternehmen, die Künstliche Intelligenz einsetzen,
stehen seit dem 2. August 2026 vor einer neuen gesetzlichen Pflicht:
Bestimmte KI-generierte Inhalte müssen klar erkennbar gemacht werden.
Was bedeutet das konkret? Was muss vorbereitet werden?

von Jessica Henning

Eine politische Rede, die nie gehalten wurde. Ein Interview, das nie stattfand. Ein Produktbild, das kein Fotostudio je aufgenommen hat. KI kann mittlerweile Inhalte erzeugen, die für das menschliche, ungeübte Auge kaum noch von der Realität zu unterscheiden sind. Wo Menschen früher sechs Finger hatten, sind nun richtigerweise fünf. Die Bild- und Mediengestaltung kann nun stärker denn je mit KI gemacht werden. Diese Entwicklung birgt erhebliche Risiken für die Allgemeinheit. Nicht nur demokratische Diskurse müssen hinterfragt werden, auch das generelle Vertrauen in Medien sinkt. Der Mensch muss eine gewisse Mündigkeit erlangen; sapere aude!

Um gegen sogenannte Deep Fakes zu wirken, begegnet der EU AI Act dieser Gefahr mit klaren Transparenzpflichten. Artikel 50 der KI-Verordnung (KI-VO) in Verbindung mit Erwägungsgrund 132 schreibt vor: Menschen sollen stets wissen können, wann sie es mit authentischen und wann mit synthetischen Inhalten zu tun haben. Ab dem 2. August 2026 gelten diese Pflichten verbindlich – für Anbieter und Betreiber von KI-Systemen gleichermaßen.

Art. 50 KI-VO im Überblick

Artikel 50 der KI-VO adressiert vier Szenarien, in denen Transparenz verpflichtend wird:

1. Direkte Interaktion mit KI (Art. 50 Abs. 1 – Anbieterpflicht): Wer KI-Systeme anbietet, die direkt mit Menschen kommunizieren, etwa Chatbots oder Sprachassistenten, muss sicherstellen, dass Nutzerinnen und Nutzer wissen, dass sie nicht mit einem Menschen, sondern mit einer Maschine, genauer gesagt mit KI, interagieren.
2. Maschinenlesbare Kennzeichnung synthetischer Inhalte (Art. 50 Abs. 2 – Anbieterpflicht): Anbieter von KI-Systemen, die Audio-, Bild-, Video- oder Textinhalte generieren, müssen deren Ausgaben in einem maschinenlesbaren Format kennzeichnen, damit sie als künstlich erzeugt erkennbar und technisch nachweisbar sind.
3. Emotionserkennung und biometrische Kategorisierung (Art. 50 Abs. 3 – Betreiberpflicht): Betreiber solcher Systeme müssen betroffene Personen informieren und DSGVO-konform handeln.
4. Deepfakes und KI-Texte von öffentlichem Interesse (Art. 50 Abs. 4 – Betreiberpflicht): Wer Deepfakes veröffentlicht oder KI-generierte Texte zu gesellschaftlich relevanten Themen publiziert, muss die künstliche Herkunft offenlegen.

Stichwort
Deepfake

Ein Deepfake ist ein durch KI (Deep Learning) erzeugter oder manipulierter Bild-, Ton- oder Videoinhalt, der täuschend echt wirkt und realen Personen, Orten oder Ereignissen ähnelt. Er kann den Eindruck erwecken, jemand sage oder tue etwas, das nie stattgefunden hat, und wird unter anderem für Täuschung und Betrug genutzt.

Art. 50 KI-VO ist keine Hochrisiko-Pflicht. Die Kennzeichnungspflichten gelten unabhängig von der Risikokategorie des eingesetzten KI-Systems für nahezu jedes Unternehmen, das KI produktiv nutzt.

Anbieter oder Betreiber? Die entscheidende Rollenunterscheidung

Wer welche Pflichten erfüllen muss, hängt maßgeblich von der Rolle des Unternehmens im KI-Ökosystem ab.

Anbieter sind Unternehmen, die ein KI-System entwickeln (oder entwickeln lassen) und es unter eigenem Namen auf den Markt bringen oder in Betrieb nehmen. Sie tragen die Verantwortung für die technische Infrastruktur, insbesondere für die maschinenlesbare Kennzeichnung aller generierten Ausgaben.

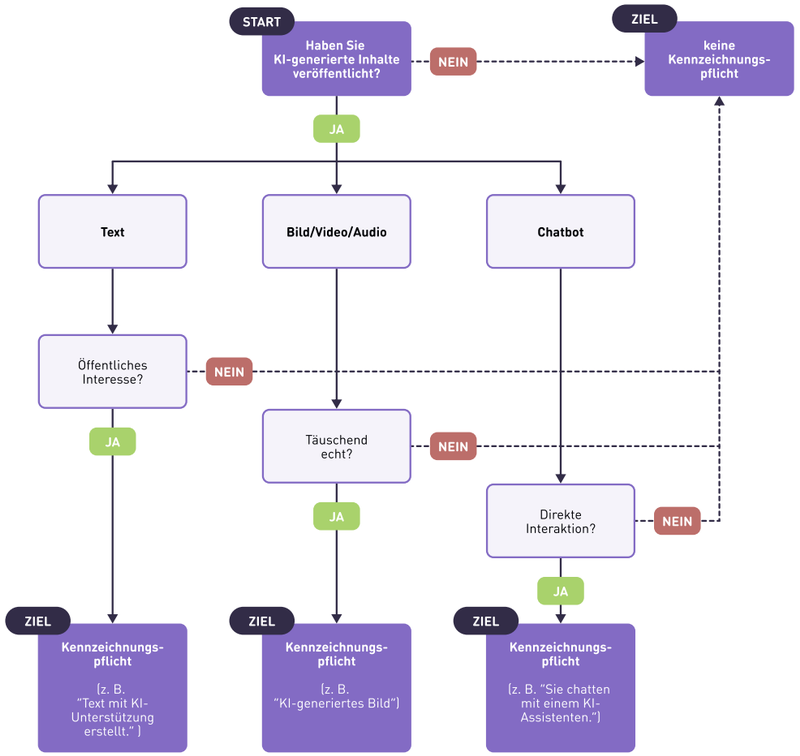
Betreiber sind Unternehmen, die bestehende KI-Systeme in eigener Verantwortung, wie etwa ChatGPT, Microsoft Copilot oder Midjourney für die Kundenkommunikation, das Marketing oder die Contenterstellung nutzen.

Ein und dasselbe Unternehmen kann beide Rollen gleichzeitig innehaben: Wer einen eigenen KI-Chatbot auf Basis eines Drittanbieter-Modells betreibt, ist gegenüber den Nutzern Anbieter (Abs. 1) und gleichzeitig Betreiber, wenn dieser Chatbot Texte zu gesellschaftlich relevanten Themen publiziert (Abs. 4).

Texte, Bilder, Videos: Wo gilt die Pflicht und wo nicht?

Nicht jeder KI-generierte Inhalt muss automatisch gekennzeichnet werden. Das Gesetz trifft bewusst Unterscheidungen:

KI-generierte Texte: Texte unterliegen der Kennzeichnungspflicht, wenn sie der „Information der Öffentlichkeit über Angelegenheiten von öffentlichem Interesse dienen“. Dies sind z. B. politische Berichte, gesellschaftliche Debatten, Nachrichten. Marketingtexte, Produktbeschreibungen, interne E-Mails oder KI-unterstützte Korrekturen fallen grundsätzlich nicht darunter. Auch ein von der KI übersetzter Text muss nicht gekennzeichnet werden, insbesondere nicht, wenn der Text sich nicht wesentlich ändert.



Bilder, Audio- und Videoinhalte (Deepfakes): Hier ist die Schwelle anders gesetzt. Kennzeichnungspflichtig sind Inhalte, die so echt oder täuschend wirken, dass ein durchschnittlicher Betrachter sie für authentisch halten könnte, insbesondere wenn sie reale Personen, Orte oder Ereignisse zeigen, die tatsächlich nicht existieren oder nicht stattgefunden haben.

Nicht kennzeichnungspflichtig sind hingegen: Rein grafische Illustrationen, Comics, Karikaturen, abstrakte Grafiken sowie Bilder, die lediglich mit unwesentlichen Korrekturen bearbeitet wurden (Schärfen, Farbkorrektur, Belichtungsanpassung).

Eine Grauzone besteht bei fotorealistischen KI-Modellen ohne reale Vorlage, etwa KI-generierten Models in Onlineshops oder virtuellen Influencern. Zwar sind diese Inhalte nicht eindeutig als Deepfakes im gesetzlichen Sinne erfasst, empfohlen wird dennoch, sie vorsorglich zu kennzeichnen. Die Kontrollfrage lautet: Könnte der durchschnittliche Betrachter davon ausgehen, dass diese Person, dieser Ort, dieses Ereignis real ist? Wenn ja – kennzeichnen.

Wie muss die Kennzeichnung aussehen?

Das Gesetz schreibt kein einheitliches Format vor, definiert aber klare Qualitätsanforderungen: Die Kennzeichnung muss klar, eindeutig und transparent sein – nicht im Fließtext versteckt, nicht in winziger Schrift am Seitenende. Sie muss barrierefrei gestaltet sein (ausreichende Kontraste, Vorlesbarkeit durch Screenreader) und spätestens bei der ersten Interaktion oder Wahrnehmung des Inhalts sichtbar sein.

Mögliche Formulierungen – je nach Kontext:
- Text: „Dieser Text wurde mit Unterstützung einer KI erstellt.“ / „KI-unterstützt erstellt.“
- Bild: „KI-generiertes Bild“ / „Dieses Bild wurde mithilfe künstlicher Intelligenz erstellt.“
- Video: „Dieses Video wurde ganz oder teilweise mit künstlicher Intelligenz erstellt.“ – als Texteinblendung am Anfang oder in der Videobeschreibung
- Audio: „Diese Audioaufnahme wurde mithilfe künstlicher Intelligenz erstellt.“ – akustischer Hinweis zu Beginn
- Chatbot: „Sie chatten mit einem KI-Assistenten.“ – direkt beim Start der Konversation, einmalige Anzeige genügt

Darüber hinaus arbeitet die Europäische Kommission an einem Verhaltenskodex zur Transparenz KI-generierter Inhalte (Code of Practice on AI-generated Content), der praktische Lösungen für die technische Umsetzung bieten soll. Für Anbieter generativer KI-Systeme ist dabei die maschinenlesbare Kennzeichnung besonders relevant. Nach dem aktuellen Entwurf sollen mindestens zwei Verfahren kombiniert werden: Digital signierte Metadaten (etwa nach dem C2PA-Standard der Coalition for Content Provenance and Authenticity) sowie unsichtbare Wasserzeichen, die auch nach Bearbeitung erhalten bleiben. Der Kodex ist zwar freiwillig. Wer ihn unterzeichnet, kann aber die darin beschriebenen Maßnahmen als Konformitätsnachweis gegenüber Behörden geltend machen.

Die EU-Kommission stellt außerdem Leitlinien sowie einen AI Act Service Desk unter *ai-act-service-desk.ec.europa.eu* bereit, der Unternehmen bei konkreten Umsetzungsfragen unterstützt.

> Für die Verpflichtung zur Einbindung eines maschinenlesbaren Wasserzeichens (Art. 50 Abs. 2 KI-VO) gilt für Systeme, die bereits vor dem 2. August 2026 in Verkehr gebracht wurden, eine Übergangsfrist zum 2. Dezember 2026.

Muss nach Risikokategorie unterschieden werden?

Das ist eine der wichtigsten und häufig missverstandenen Fragen in der Praxis. Die Antwort: Nein.

Die Transparenz- und Kennzeichnungspflichten nach Art. 50 KI-VO gelten unabhängig von der Risikokategorie des eingesetzten KI-Systems. Ein Unternehmen muss seinen KI-Chatbot auch dann kennzeichnen, wenn er in keine Hochrisiko-Kategorie fällt. Ein fotorealistisches, KI-generiertes Produktbild muss auch dann offengelegt werden, wenn das dahinterstehende KI-System als „geringes Risiko“ eingestuft ist.

Dies unterscheidet Art. 50 fundamental von den meisten anderen Anforderungen des AI Act, die sich an der Risikoeinstufung orientieren. Die Transparenzpflicht ist ein horizontaler Querschnitt durch alle Risikostufen, weil das Täuschungspotenzial nicht vom Risiko des Systems, sondern von der Wirkung auf den Rezipienten abhängt.

Die Risiken bei Nicht-Einhaltung

Wer die Kennzeichnungspflichten ignoriert oder schlicht nicht kennt, riskiert empfindliche Konsequenzen:

Bußgelder: Verstöße gegen Art. 50 fallen unter die zweite Sanktionsstufe der KI-Verordnung (Art. 99 KI-VO). Die Geldbußen betragen bis zu 15 Millionen Euro oder bei Unternehmen 3 Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. KMU und Startups erhalten bei der Bemessung zwar besondere Berücksichtigung und nach dem aktuellen Stand des Digital Omnibus sogar eine automatische Reduktion von 50 Prozent für KMU bzw. 75 Prozent für Kleinstunternehmen. Das ändert aber nichts an der grundsätzlichen Pflicht.

Reputationsschäden: Noch schwerer als das Bußgeld kann für viele Unternehmen der Vertrauensverlust wiegen. Wer mit KI-Inhalten täuscht, bewusst oder unbeabsichtigt, riskiert öffentliche Kritik, Medienberichte und den Verlust von Kundenvertrauen. In einer Zeit, in der Authentizität zum Markenwert wird, ist Transparenz auch eine strategische Entscheidung.

Wettbewerbsrechtliche Risiken: Irreführende Geschäftspraktiken können zusätzlich wettbewerbsrechtlich verfolgt werden, parallel zur KI-VO.

Was Unternehmen jetzt konkret tun sollten

Wer strukturiert vorgeht, kann die Anforderungen mit vertretbarem Aufwand umsetzen. Folgende Schritte sind empfehlenswert:

1. **Bestandsaufnahme: KI-Inventar erstellen**
   Welche KI-Systeme werden im Unternehmen eingesetzt? Wo entstehen dadurch Inhalte, die nach außen

Ausnahmen von der Kennzeichnungspflicht:

- **Texte:** Wenn ein Mensch die redaktionelle Verantwortung übernimmt und die inhaltliche Prüfung dokumentiert ist; bei rein internen oder privaten Inhalten; wenn KI nur korrigiert oder übersetzt
- **Deepfakes:** Wenn der Inhalt offensichtlich künstlerischen, satirischen oder fiktionalen Charakter hat – soweit die Kennzeichnung das Werk beeinträchtigen würde; bei nicht irreführenden Inhalten
- **Bilder:** Wenn nur unwesentliche Bearbeitungen vorgenommen wurden (Farbkorrektur, Schärfe, Belichtung)

kommuniziert werden? Ein zentrales KI-Verzeichnis, das Systeme, Anwendungsfälle und Verantwortlichkeiten dokumentiert, ist die Basis für alles Weitere.

2. Rollenklärung: Anbieter oder Betreiber?
Für jedes System ist zu klären, welche Rolle das Unternehmen einnimmt und welche Pflichten daraus folgen. Beides kann gleichzeitig zutreffen.

3. Inhaltliche Bewertung: Was ist kennzeichnungspflichtig?
Nicht alle KI-Inhalte sind betroffen. Für jeden Anwendungsfall ist zu prüfen: Handelt es sich um einen Deepfake? Adressiert der Text ein Thema von öffentlichem Interesse? Interagiert das System direkt mit Menschen?

„Wer strukturiert vorgeht, kann die Anforderungen mit vertretbarem Aufwand umsetzen."

4. Prozesse anpassen: Kennzeichnung einbauen und Ausnahmen nutzen.
Wo Kennzeichnungspflicht besteht, braucht es klare Prozesse und Standardformulierungen für Text, Bild, Video, Audio; technische Umsetzung im CMS, in Social-Media-Tools, im E-Mail-Marketing. Wo eine menschliche redaktionelle Prüfung dokumentiert wird, kann die Pflicht unter Umständen entfallen. Prozesse sollten auch diese Ausnahmen systematisch abbilden.

5. Dokumentation sicherstellen
Sowohl die Kennzeichnung selbst als auch die Entscheidung, nicht zu kennzeichnen, sollte dokumentiert sein als Nachweis gegenüber Aufsichtsbehörden und als Grundlage interner Prüfprozesse.

Fazit: Kennzeichnung ist mehr als Compliance

Artikel 50 der KI-Verordnung ist kein technisches Detailproblem für Entwicklungsabteilungen. Er ist eine Querschnittspflicht, die Marketing, Kommunikation, Rechtsabteilung und IT gleichermaßen betrifft.

Die Anforderungen sind klar genug, um heute zu handeln, auch wenn einzelne Details, wie die genaue technische Umsetzung der Wasserzeichenpflicht, noch durch den Verhaltenskodex der EU-Kommission weiter konkretisiert werden.

Unternehmen, die die Kennzeichnungspflicht jetzt strukturiert angehen, profitieren doppelt: Sie vermeiden Sanktionen und Reputationsschäden und sie positionieren sich als vertrauenswürdige Akteure in einer Zeit, in der der Umgang mit KI zum Spiegel unternehmerischer Verantwortung wird. &

Impressum

Redaktion/V. i. S. d. P.:
Torben Paradiek,
Thomas Althammer

Haftung und Nachdruck:
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.

Schutzgebühr Print-Ausgabe: 5,– €

Gestaltung:
Designbüro Winternheimer, *winternheimer.net*

Fotos Mini-Figuren:
Katja Borchhardt, *miniansichten.de*

Anschrift:
Althammer & Kill GmbH & Co. KG
Roscherstraße 7 · 30161 Hannover
Tel. +49 511 330603-0
althammer-kill.de

Die Menschen bei Althammer & Kill:

Charlene Engelhardt

Ja hallo, wer bist Du denn?

Charlene Engelhardt: Ich bin Charlene und lebe seit sechs Jahren in Hannover. Seit Januar 2025 bin ich bei A&K als Marketing Managerin mit Schwerpunkt Online-Marketing tätig. Vielleicht kennt der eine oder andere mein Gesicht aus dem Newsletter.

Wie bist du auf Althammer & Kill aufmerksam geworden?

Charlene Engelhardt: Mein vorheriger Arbeitgeber war bereits Kunde von A&K, daher kannte ich das Unternehmen. Als mich eine Kollegin auf die Stellenausschreibung aufmerksam machte, habe ich mich kurz vor Weihnachten beworben. Danach ging alles ziemlich schnell: Probeaufgabe, ein sehr angenehmes Gespräch mit Thomas und Nina und bereits kurz nach Neujahr die Zusage. Der gesamte Prozess dauerte nicht einmal zwei Wochen. Damit hatte ich wirklich nicht gerechnet.

Was sind deine Aufgaben bei Althammer & Kill?

Charlene Engelhardt: Meinen Arbeitsalltag verbringe ich hauptsächlich vor dem Rechner. Da meine Aufgaben sehr abwechslungsreich und vielfältig sind, gleicht kaum ein Tag dem anderen. Mal sitze ich einen halben Tag in Meetings, mal pflege ich Inhalte auf unserer Website ein oder beschäftige mich mit SEO und dem Controlling. An anderen Tagen arbeite ich an unseren Newslettern oder bereite Veranstaltungen vor. Ein weiterer Schwerpunkt meiner Arbeit ist LinkedIn. Die meisten Beiträge, die auf unserem Unternehmensprofil erscheinen, stammen von mir. Außerdem verantworte ich verschiedene Newsletter, darunter das Compliance Update, unseren internen Newsletter „Insider" sowie den LinkedIn-Newsletter. Besonders viel Freude bereitet mir die Planung und Moderation unserer Webinare und Seminare. Vor allem Kooperationsveranstaltungen, beispielsweise mit Connext Vivendi, machen mir großen Spaß. Doch nicht nur Online-Formate gehören zu meinem Aufgabenbereich: Auch die Organisation und Begleitung von Präsenzveranstaltungen ist ein wichtiger Teil meiner Arbeit. Mein persönliches Herzensprojekt ist das KI-Forum, das im nächsten Jahr bereits zum dritten Mal stattfinden wird. Darüber hinaus bin ich für die Planung und Beschaffung unserer Give-aways sowie der Printmedien verantwortlich, die wir auf Veranstaltungen einsetzen. Dabei arbeite ich eng mit unserem externen Grafiker sowie weiteren externen Dienstleistern zusammen und stehe natürlich auch im regelmäßigen Austausch mit meinen Kolleginnen und Kollegen.

Wie ist das Arbeiten in Bezug auf Datenschutz für dich?

Charlene Engelhardt: Spannend, denn die Herausforderung ist, Datenschutz auch mal „sexy" zu vermarkten. Gleichzeitig begegnet mir das Thema täglich, etwa bei Kontaktformularen, Newslettern oder Webinaren. Oft muss eine kreative Idee noch einmal angepasst werden, damit sie auch datenschutzkonform funktioniert. Genau dieser Spagat macht die Arbeit für mich interessant.

Was gefällt dir besonders an der Arbeit?

Charlene Engelhardt: Der Austausch mit meinen Kolleginnen und Kollegen und externen Partnern, die abwechslungsreichen Aufgaben und die Freiheit, meinen Arbeitsalltag eigenständig zu strukturieren.
Ein Highlight sind außerdem unsere Teamtage. Da wir an verschiedenen Standorten arbeiten, ist es umso schöner, sich persönlich zu treffen und gemeinsam Zeit zu verbringen.

Wann war deine Arbeit erfolgreich?

Charlene Engelhardt: Wenn sie einen spürbaren Beitrag leistet, zum Beispiel durch neue Leads, erfolgreiche Beiträge oder gut besuchte Veranstaltungen. Besonders schön finde ich es, wenn aus digitalen Zahlen echte Begegnungen werden. Beim KI-Forum wird das besonders greifbar: Menschen kommen zusammen, tauschen sich aus und nehmen neue Impulse mit. Dann weiß ich, dass unsere Arbeit Wirkung zeigt.

Was machst du, wenn du nicht arbeitest?

Charlene Engelhardt: Ich lese sehr gerne und verbringe viel Zeit mit Freunden, zum Beispiel bei gemeinsamen Kochabenden oder spontanen Unternehmungen. Und dann gibt es noch meine persönlichen „Grandma Hobbys": Sticken und Häkeln. Was soll ich sagen? Ich mag es einfach, Dinge zu erschaffen. &

Compliance bei Startups – besser aus der Not eine Tugend machen

Datenschutz, Informationssicherheit und KI-Regulierung gleich mitzudenken vermeidet böses Erwachen und schafft Vertrauen beim Kunden.

von Dr. Martin Mühlpfordt

In der Natur von Startups liegt es, zur innovativen Kernidee möglichst schnell ein erstes Produkt auf den Markt zu bringen. Auf schmückendes Beiwerk wird dabei erst einmal verzichtet. Nur sollte man sich davor hüten, auch Datenschutz, Informationssicherheit und KI-Regulatorik auf später zu verschieben.

Im B2B-Bereich erwarten Kunden von ihren Dienstleistern einen professionellen Umgang mit Compliance-Fragen. Aber welche Compliance-Aspekte sollten Startups wann betrachten?

Zentrale Compliance-Bereiche für Startups

Neben den Anforderungen aus dem Gesellschafts-, Handels- und Steuerrecht sollten bei einer geplanten Unternehmensgründung drei wichtige Compliance-Bereiche beachtet werden: Datenschutz, Informationssicherheit und die Regulierung von KI-Systemen.

Datenschutz betrifft den Umgang mit personenbezogenen Daten und ist durch die DSGVO europaweit geregelt. Sofern die geplante Dienstleistung die Verarbeitung

personenbezogener Daten der Kunden beinhaltet, so muss im B2B-Umfeld die Rolle eines Auftragsverarbeiters unbedingt verinnerlicht werden.

Informationssicherheit schützt alle geschäftskritischen Informationen vor Verlust, Manipulation oder unbefugtem Zugriff. Für den Datenschutz ist es das technische und organisatorische Fundament. Und je nach Branche werden Dienstleister von ihren Kunden zunehmend kritisch unter die Lupe genommen.

KI-Regulierung folgt aus der EU-KI-Verordnung. Sofern künstliche Intelligenz ein wichtiges Element im Produkt werden soll, müssen Anbieterpflichten erfüllt werden. Diese hängen vom Risikograd des KI-Einsatzes ab.

Datenschutz: Rollenverständnis verinnerlichen

Im B2B-Bereich agieren Startups häufig als Auftragsverarbeiter, z. B. wenn Kunden mit einem geplanten Cloud-Produkt personenbezogene Daten verarbeiten. Wichtig ist hierbei zu verstehen, dass die Kundendaten nicht „unsere Daten“ des Startups sind. Sie dürfen ausschließlich für die Dienstleistungserbringung verarbeitet werden. Eine Weiterverwendung zu eigenen Zwecken, wie Marketing, Nutzungsanalysen oder als Testdatensatz für die nächste Produktversion, ist ausgeschlossen.

Die strikte Unterscheidung von Kunden- und den eigenen Daten, der Verarbeitung für den Kunden und der für eigene Zwecke sollte bereits in der Ideenphase verstanden und mitgedacht werden und dann Teil der Unternehmenskultur werden.

Dieses Selbstverständnis als Auftragsverarbeiter hilft später bei der Entwicklung des „Minimum Viable Products“ (MVP), um die Grundsätze „Privacy by Design“ und „Privacy by Default“ aus Kundensicht greifbar zu machen. Angemessene technische und organisatorische Sicherungsmaßnahmen sollten geplant und nach und nach im Produkt umgesetzt werden. Auch hier gilt: Tue Gutes und sprich darüber! Kunden benötigen später eine Dokumentation dieser Maßnahmen.

Für die weitere Professionalisierung, die häufig auf Fremdkapital angewiesen ist, reicht die Datenschutzkonformität des Produkts allein nicht aus. Kunden werden Unterstützung bei der Erfüllung ihrer datenschutzrechtlichen Pflichten einfordern: ein ausgewogener Auftragsverarbeitungsvertrag, gute Vorlagen und Materialien für Daten-

Ist Ihr Startup Enterprise-Ready?

Ihr Produkt überzeugt, die Demo läuft gut, der Entscheider ist an Bord. Und dann meldet sich die Rechtsabteilung. Plötzlich geht es nicht mehr um Features, sondern um Datenschutz, Informationssicherheit und Compliance. Wer als Startup mit Konzernen, Banken oder öffentlichen Institutionen ins Geschäft kommen möchte, muss deshalb mehr bieten als ein gutes Produkt. Enterprise-Kunden wollen wissen, ob ein Anbieter auch organisatorisch und regulatorisch ein verlässlicher Partner ist. Drei Themen werden dabei besonders wichtig:

1. Datenschutz schafft Vertrauen
Wie werden personenbezogene Daten verarbeitet? Gibt es klare Regelungen zur Auftragsverarbeitung? Sind Unterdienstleister transparent dokumentiert und Lösch-, Zugriffs- sowie Meldeprozesse definiert? Wer diese Fragen schnell und nachvollziehbar beantworten kann, erleichtert seinen Kunden die Prüfung – und beschleunigt im besten Fall den Sales-Prozess.

2. Informationssicherheit braucht Nachweise
Spätestens mit dem ersten Vendor-Fragebogen zeigt sich, wie gut ein Startup vorbereitet ist. Standards wie ISO 27001, IT-Grundschutz oder branchenspezifische Anforderungen spielen im Enterprise-Umfeld eine wichtige Rolle. Nicht jedes Startup benötigt sofort eine Zertifizierung. Ein IS-Check oder eine GAP-Analyse kann aber früh zeigen, welche Anforderungen relevant sind und wo Handlungsbedarf besteht.

3. KI-Compliance wird zum Verkaufsfaktor
Setzt das eigene Produkt KI ein, kommen neue Fragen hinzu: Welche KI-Systeme werden genutzt? Welche Risiken bestehen? Wie transparent sind Datenverarbeitung und Training? Und welche Anforderungen ergeben sich aus der EU-KI-Verordnung? Wer darauf vorbereitet ist, reduziert Unsicherheit auf Kundenseite.

Der beste Zeitpunkt für diese Themen ist nicht der erste Enterprise-Deal, sondern die Produktentwicklung. Compliance by Design reduziert spätere Nacharbeiten, erleichtert Due-Diligence-Prozesse und schafft Vertrauen bei Kunden, Partnern und Investoren. Startups müssen dabei nicht alles auf einmal lösen. Entscheidend ist, früh zu wissen, wo man steht, was der Zielmarkt erwartet und welche Maßnahmen den größten Hebel haben. Denn Enterprise-ready bedeutet nicht, perfekt zu sein, sondern vorbereitet.

KLICK/SCAN

schutzhinweise, Verarbeitungsverzeichnisse und Datenschutz-Folgenabschätzungen helfen dabei, schneller ins Geschäft zu kommen.

Informationssicherheit: Frühzeitig Kundenanforderungen kennen

Die primären Schutzziele der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Auch hierbei ist es sinnvoll, die Sphäre der Kunden- und der eigenen Informationen separat zu betrachten. Auf das Produkt bezogen gibt es dabei große Überschneidung mit den Sicherungsmaßnahmen für den Datenschutz.

Soll das Minimum Viable Product mehr als ein Demonstrator sein, also bereits beim Kunden in den produktiven Einsatz gehen, muss es den Stand der Technik erfüllen. Startups sollten sich hierfür z. B. mit den relevanten Bausteinen aus dem BSI-IT-Grundschutz vertraut machen. In bestimmten Branchen gelten auch strengere Regeln, z. B. für Betreiber kritischer Infrastruktur, im Gesundheitswesen oder der Automobilindustrie, die dann als umfangreiche Anforderungen an die Lieferanten und Dienstleister weitergereicht werden. Dies muss beim Erstellen des Geschäftsplanes bekannt sein.

„Im B2B-Bereich erwarten Kunden von ihren Dienstleistern einen professionellen Umgang mit Compliance-Fragen."

KI-Einsatz: Hoch-Riskantes als Selling Point – oder aber vermeiden

Die KI-Verordnung der EU ist ein Produktsicherheitsgesetz und reguliert den Einsatz von KI mit einem risikobasierten Ansatz. Die mit einem unannehmbaren Risiko verbundenen KI-Praktiken sind seit 2025 verboten. Andere Einsatzgebiete von KI-Systemen werden als hochriskant eingeschätzt. Auf Anbieter solcher Systeme kommen ab Ende 2027 umfangreiche Aufgaben zu, wie Aufbau und Pflege eines Risikomanagementsystems, Erfüllung von Dokumentations-, Aufzeichnungs-, Transparenzpflichten und nicht zuletzt das Absolvieren eines Konformitätsbewertungsverfahren.

Will ein Startup in den Hoch-Risiko-Bereich gehen, dann wird der professionelle Umgang mit diesen Compliance-Anforderungen ein zentrales Element der Geschäftsidee sein, denn deren Erfüllung wird mit großen Aufwänden verbunden sein.

Alle anderen Startups, die KI im Produkt einbauen möchten, sollten sich Gewissheit darüber verschaffen, dass sie nicht der Hoch-Risiko-Regulatorik unterliegen. Dies sollte in einer nachvollziehbaren Risikoeinschätzung dokumentiert werden, denn auch Kunden werden danach fragen.

Fazit: Den richtigen Zeitpunkt beachten

Es gilt die Binsenweisheit „Vorsorge ist besser als Nachsorge". Die beschriebenen Maßnahmen erfordern Handeln an verschiedenen Zeitpunkten im Gründungsprozess. Hier eine grobe Orientierung für den richtigen Zeitpunkt:

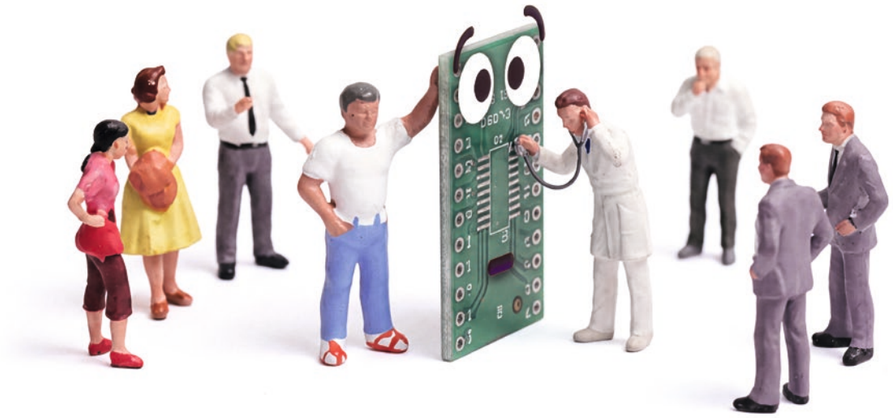
Ideenphase: Datenschutzrechtliche Rolle klären, KI-Risikoklasse prüfen, branchenspezifische Sicherheitsanforderungen identifizieren.

Gründungsphase: Privacy by Design und Privacy by Default umsetzen. Grundlegende Sicherheitsmaßnahmen nach Stand der Technik und Branchenanforderung implementieren. KI-Risikoklassifikation dokumentieren, bei Hochrisiko-KI Compliance-System aufbauen.

Markteintritt: Datenschutzdokumente für Kunden bereithalten, Informationssicherheitskonzept dokumentieren, bei KI-Produkten Transparenzpflichten prüfen.

Wachstumsphase: Datenschutzbeauftragten bestellen, Informationssicherheitssystem aufbauen, Zertifizierungen anstreben (z. B. ISO 27001).

Compliance ist somit keine einmalige Aufgabe, die man später noch erledigen kann. Werden rechtliche Anforderungen rechtzeitig erkannt, können Geschäftsidee und Produkteigenschaften angepasst und Zusatzaufwände in den Finanzierungsbedarf eingeplant werden. &



Der EU-Leitlinien-Entwurf zur KI-Risikoeinstufung

Am 19. Mai 2026 hat die Europäische Kommission den lang erwarteten Entwurf der Leitlinien zur Einstufung von Hochrisiko-KI-Systemen veröffentlicht. Schon jetzt bietet der Entwurf Unternehmen ein konkretes Werkzeug, um Risiken besser einschätzen zu können.

von Jessica Henning

In den vergangenen Monaten kam wohl in jedem zweiten Compliance-Meeting Fragen auf wie „Ist unser KI-System eigentlich Hochrisiko?" oder „Was müssen wir für Pflichten beachten?". Der Gesetzestext von Artikel 6 der KI-VO lieferte die juristische Grundlage, aber keine anwendbare Methodik. Unternehmen bewegten sich im Interpretationsspielraum, Datenschützer mahnten zur Vorsicht, und Behörden hatten noch keine einheitliche Linie.

Ziel des Entwurfes

Um dies zu ändern hat die Europäische Kommission am 19. Mai 2026 den Entwurf der Leitlinien zur Klassifizierung von Hochrisiko-KI-Systemen gemäß Artikel 6 AI Act zur Konsultation veröffentlicht. Die Leitlinie ist kein weiteres abstraktes behördliches Papier, sondern eines der ersten praxisorientierten Instrumente, das Anbietern, Betreibern und Aufsichtsbehörden eine nachvollziehbare, einheitliche Methodik zur Hand gibt.

> „Diese Leitlinien zielen darauf ab, Anbieter und Betreiber von KI-Systemen sowie die zuständigen Marktüberwachungsbehörden bei der Beurteilung zu unterstützen, ob ein KI-System als hochriskant eingestuft werden sollte, und erleichtern so die einheitliche Anwendung und wirksame Durchsetzung von Artikel 6 AI Act."*

KLICK/SCAN

Europäische Kommission, Draft Guidelines on the Classification of High-Risk AI Systems pursuant to Article 6 AI Act, May 2026

Die zwei Säulen der Hochrisiko-Einstufung

Der Entwurf strukturiert die Klassifizierung entlang zweier klar getrennter Szenarien, die auf Artikel 6 KI-VO basieren:

Säule 1 – Artikel 6 Absatz 1 + Anhang I der KI-VO: Regulierte Produkte

KI-Systeme, die selbst ein Produkt nach EU-Harmonisierungsrecht sind oder als Sicherheitskomponente in einem solchen Produkt eingesetzt werden, gelten als hochriskant; sofern das betreffende Produkt einer verpflichtenden Drittpartei-Konformitätsbewertung unterliegt. Darunter fallen etwa Maschinen, Medizinprodukte, Spielzeug oder Fahrzeugkomponenten. Entscheidend ist dabei nicht das Produkt selbst, sondern ob es in der Harmonisierungsgesetzgebung des Anhangs I der KI-VO gelistet ist. Eine Sicherheitskomponente ist dabei definiert als ein Bestandteil, dessen Ausfall oder Fehlfunktion die Gesundheit oder Sicherheit von Personen gefährden würde.

Säule 2 – Artikel 6 Absatz 2 + Anhang III der KI-VO: Eigenständige KI-Systeme

Hier werden eigenständige KI-Systeme erfasst, die in bestimmten, von der Verordnung als besonders risikobehaftet eingestuften Bereichen eingesetzt werden. Die Leitlinien listen acht übergeordnete Kategorien auf, die laut Anhang III als besonders anfällig für Risiken gelten.

Die acht Hochrisiko-Bereiche nach Anhang III:

1. Fernidentifikation, Kategorisierung, Emotionserkennung
2. Kritische Infrastruktur (Strom, Wasser, Gas, Verkehr, digitale Infrastruktur)
3. Bildung und Berufsausbildung (Zulassung, Lernbewertung, Prüfungsüberwachung)
4. Beschäftigung (Recruiting, Leistungsbeurteilung, Personalsteuerung)
5. Wesentliche Dienste (Kreditwürdigkeit, Sozialleistungen, Notfallpriorisierung, Versicherung)
6. Strafverfolgung (Opferrisikoanalyse, Lügendetektoren, Beweisbewertung)
7. Migration und Asyl (Grenzkontrolle, Risikoeinschätzung, Antragsbearbeitung)
8. Justiz und Demokratie (Justizunterstützung, Wahlbeeinflussung)

Konkrete Beispiele im Entwurf

Der eigentliche Mehrwert des Entwurfs liegt in seinen illustrativen Praxisbeispielen. Die Kommission stellt für jeden Bereich konkrete Anwendungsfälle vor und beantwortet jeweils, ob ein System als hochriskant eingestuft wird oder nicht. Dabei gilt ausdrücklich: Die Beispielliste ist nicht abschließend, sondern ein dynamisches Instrument, das kontinuierlich aktualisiert wird. Ähnlich wie die von den Datenschutzaufsichtsbehörden veröffentlichten Listen typischer DSFA-Fälle (sog. „Muss-Listen") bieten diese Beispiele Orientierung für die praktische Einordnung.

Eine oft geführte Diskussion ist folgendes Beispiel: Eine Smartwatch erkennt per Herzschlag-Tracking eine Emotion. Dies gilt nach dem Entwurf der Europäischen Kommission als Hochrisiko-Anwendung. Emotionserkennung über biometrische Daten ist kein harmloses Feature, sie fällt unter die strengen Auflagen des Biometrie-Bereichs.

Ein weiteres wichtiges Klarstellungsbeispiel aus dem Beschäftigungsbereich: KI-gestützte Lebenslauf-Screening-Tools sind hochriskant, wenn sie an der finalen Auswahlentscheidung beteiligt sind. Systeme, die lediglich vorbereitend tätig sind und die menschliche Entscheidung inhaltlich nicht strukturieren, können unter bestimmten Umständen aus der Hochrisiko-Klassifizierung herausfallen.

Schließung von Auslegungen

Der Entwurf adressiert auch zwei verbreitete Missverständnisse in der Compliance-Praxis, die in der Vergangenheit als argumentative Ausfluchten genutzt wurden:

1. „Wir haben einen Menschen im Prozess"

Die Leitlinien stellen klar: Menschliche Beteiligung allein verändert die Risikobewertung nicht. Wer formal einen Menschen an das Ende einer KI-Entscheidungskette setzt, ohne dass dieser tatsächlich die Ausgabe inhaltlich überprüfen kann, hat keine Handhabe zur Herabstufung. Menschliche Aufsicht ist als eine Voraussetzung für bereits eingestufter Hochrisiko-Systeme anzusehen und nicht als Strategie zur Vermeidung der Einstufung.

2. „Wir haben in den Nutzungsbedingungen Hochrisiko-Nutzung ausgeschlossen"

Die rein vertragliche Ausgrenzung von Hochrisiko-Anwendungsfällen wurde ebenfalls aufgegriffen. Der Entwurf hält unmissverständlich fest: Wenn ein System technisch für Hochrisiko-Zwecke geeignet ist und dies angesichts seiner Funktionalitäten vernünftigerweise vorhersehbar ist, reicht ein pauschaler Ausschluss in den AGBs nicht aus. Anbieter müssen Nutzungsbeschränkungen klar, konkret und konsistent in allen Unterlagen kommunizieren.

Regelung	Ursprüngliches Datum	Nach KI-Omnibus
Hochrisiko-Systeme (Anhang III, Art. 6 Abs. 2).	2. August 2026	**2. Dezember 2027**
Hochrisiko-Produkte (Anhang I, Art. 6 Abs. 1)	2. August 2027	**2. August 2028**
Öffentliche Stellen: alle Hochrisiko-Systeme	—	**2. August 2030**

Neuer Anwendungszeitplan nach KI-Omnibus

Der „Filter-Mechanismus" – Ausnahmen mit engen Grenzen

Artikel 6 Absatz 3 KI-VO sieht einen sogenannten Filter vor. KI-Systeme, die zwar unter einen Anhang-III-Bereich fallen, aber keine erheblichen Risiken darstellen, können von der Hochrisiko-Klassifizierung ausgenommen werden. Der Entwurf legt jedoch enge Bedingungen fest:

- Das System erfüllt nur rein prozedurale oder vorbereitende Aufgaben.
- Das System verbessert lediglich eine bereits abgeschlossene menschliche Handlung.
- Die Ausgaben des Systems haben keine direkten Auswirkungen auf die betroffene Entscheidung.

Dieser Filter darf unter keinen Umständen als Freifahrtschein angesehen werden. Die Kommission betont ausdrücklich, dass die Bedingungen eng auszulegen sind und eine einfache Erklärung, man habe einen Menschen eingebunden, nicht ausreicht.

Timeline: Wann gelten die Hochrisiko-Pflichten?

Der Entwurf präzisiert auch den Anwendungszeitplan – angepasst durch den KI-Omnibus, der am 27. Juli 2026 in Kraft trat: Die verschobenen Fristen bieten Unternehmen mehr Zeit zur Etablierung der neuen Compliance-Vorschriften und eine Klassifizierung schon eingesetzter KI-Systeme.

Was Unternehmen jetzt tun müssen

Auf Basis des Leitlinien-Entwurfs lassen sich fünf konkrete Handlungsschritte ableiten:

1. Selbsteinstufung strukturiert durchführen:
Prüfen Sie jedes eingesetzte oder geplante KI-System anhand der Anhang-I-Produktliste und der acht Anhang-III-Kategorien. Der Leitlinien-Entwurf bietet dafür erstmals eine belastbare Methodik.

2. Geplanter Einsatzzweck sorgfältig dokumentieren:
Der Zweck des Systems ist der entscheidende Klassifizierungsparameter, insbesondere bei KI-Systemen mit allgemeinem Verwendungszweck. Der Einsatzzweck muss in der Dokumentation konsistent und eindeutig beschrieben sein.

3. Filter-Ausnahmen kritisch überprüfen:
Wenn Sie bislang davon ausgegangen sind, dass Ihr System dank menschlicher Beteiligung oder vertraglicher Ausschlüsse aus der Hochrisiko-Kategorie herausfällt, sollten Sie diese Annahme jetzt anhand des Entwurfs neu bewerten.

4. Klassifizierungsentscheidungen dokumentieren:
Halten Sie Ihre Einstufungsentscheidung schriftlich fest, mit direktem Bezug auf die relevanten Passagen der Leitlinien. Diese Dokumentation kann bei späteren Prüfungen durch die Marktüberwachungsbehörde sehr wertvoll sein.

5. Den Konsultationsprozess aktiv nutzen:
Der Entwurf befindet sich noch in der Stakeholder-Konsultation. Unternehmen und Verbände haben die Möglichkeit, Feedback einzubringen und die finale Fassung mitzugestalten – eine Chance, die strategisch genutzt werden sollte.

Fazit: Ein Kompass für die KI-Compliance

Der Leitlinien-Entwurf der Europäischen Kommission zur Hochrisiko-Klassifizierung ist mehr als ein Interpretationsdokument. Er ist ein Praxishandbuch, das Unternehmen endlich in die Lage versetzt, ihre KI-Systeme rechtssicher, nachvollziehbar und einheitlich einzustufen. Wer den Entwurf jetzt ernst nimmt, schafft nicht nur Compliance – er schafft Vertrauen.

Die Konsultationsphase ist die letzte Gelegenheit, auf die finale Fassung Einfluss zu nehmen. Die Zeit danach gehört der Umsetzung. &

Der Cyber Resilience Act – neue Anforderungen für digitale Produkte

Mit dem Cyber Resilience Act (CRA) schafft die Europäische Union eine Rechtsgrundlage zur Cybersicherheit bei digitalen Produkten oder Produkten mit digitalen Elementen.

von Okka Jenssen

Die Verordnung verpflichtet Unternehmen, Cybersicherheit bereits während der Entwicklung eines Produkts zu berücksichtigen („Security by Design“) und diese über dessen gesamten Lebenszyklus sicherzustellen.

Ab dem 11. September 2026 gelten Meldepflichten für aktiv ausgenutzte Schwachstellen. Ab dem 11. Dezember 2027 müssen neue oder wesentlich veränderte Produkte mit digitalen Elementen die Vorschriften des CRA erfüllen. Es müssen u. a. Sicherheitsupdates bereitgestellt, eine CE-Kennzeichnung getragen und eine Software Bill of Materials (SBOM) vorgehalten werden.

Da mittlerweile ein Großteil der Verarbeitung personenbezogener Daten mithilfe digitaler Produkte durchgeführt wird, wird der CRA auch die praktische Umsetzung der DSGVO im Rahmen der technischen und organisatorischen Maßnahmen nachhaltig beeinflussen.

Welche Produkte und Unternehmen sind betroffen?

Der CRA gilt grundsätzlich für alle Produkte mit digitalen Elementen, die in der Europäischen Union in Verkehr gebracht werden und mit einem Gerät oder Netzwerk kommunizieren können. Hierzu zählen beispielsweise Hard- und Software, Smart-Home-Produkte, mobile Anwendungen, VPN-Lösungen oder bestimmte Cloud-Dienste, sofern diese als Datenfernverarbeitungslösung Bestandteil eines Produkts sind.

Neben den Herstellern sind auch Importeure, Händler, Bevollmächtigte sowie Unternehmen, die digitale Komponenten in eigene Produkte integrieren oder unter eigenem Namen vertreiben, betroffen und müssen daher die Anforderungen des CRA erfüllen. Ob ein Unternehmen vom CRA betroffen ist, hängt daher maßgeblich davon ab, ob es betroffene Produkte herstellt oder vertreibt. Reine Dienstleistungen sind dagegen grundsätzlich nicht CRA-relevant.

Für einzelne Branchen (etwa Medizinprodukte, Kraftfahrzeuge oder die Luftfahrt) gelten spezielle europäische Regelungen, sodass diese Bereiche vom CRA ausgenommen sind. Die Bereichsausnahmen sind unter Art. 2 CRA aufgelistet.

Abgrenzung zwischen Produkt und Dienstleistung

Ob ein Angebot als digitales Produkt bzw. Produkt mit digitalen Elementen oder als Dienstleistung einzustufen ist, hängt maßgeblich davon ab, ob dem Kunden eine Software oder Hardware zur Nutzung bereitgestellt wird oder lediglich ein vom Anbieter betriebener Online-Dienst. Installierbare Software, Apps oder On-Premises-Lösungen sind regelmäßig Produkte mit digitalen Elementen und können unter den CRA fallen.

Reine Cloud- oder SaaS-Dienste, wie z. B. Ticket-, Buchhaltungs- oder HR-Systeme, die ausschließlich über den Browser oder eine vom Anbieter betriebene Infrastruktur genutzt werden, sind regelmäßig digitale Dienstleistungen und fallen daher nicht in den Anwendungsbereich des CRA. Sie werden vielmehr durch andere Regelwerke, etwa die NIS-2-Richtlinie oder nationale IT-Sicherheitsvorschriften, erfasst.

Neue Anforderungen an Sicherheit und Compliance

Der CRA konkretisiert die bislang eher abstrakten Sicherheitsanforderungen der DSGVO. Unternehmen, die Produkte mit digitalen Elementen vertreiben oder entwickeln und auf dem EU-Markt bereitstellen, müssen künftig nachweisen können, dass diese Produkte den gesetzlichen Cybersicherheitsanforderungen entsprechen. Hierzu gehören unter anderem eine technische Dokumentation, eine SBOM, Konformitätsbewertungen, CE-Kennzeichnung sowie ein dokumentiertes Schwachstellenmanagement.

Besonders relevant ist der dem CRA zugrunde liegende Lebenszyklusansatz. Hiernach müssen Hersteller Risiken bereits während der Entwicklung analysieren, Drittkomponenten sicher integrieren, Sicherheitsupdates bereitstellen und Schwachstellen kontinuierlich überwachen sowie melden.

Risikoklassen bestimmen den Umfang der Anforderungen

Der CRA verfolgt einen risikobasierten Ansatz und unterscheidet zwischen regulären, wichtigen und kritischen Produkten mit digitalen Elementen (Art. 6–8 CRA). Während für alle Produkte die grundlegenden Sicherheitsanforderungen nach Anhang I gelten, unterliegen wichtige und insbesondere kritische Produkte weitergehenden Konformitätsbewertungsverfahren und teilweise zusätzlichen Nachweispflichten. Die zutreffende Einstufung eines Produkts ist daher der wesentliche Schritt für die Umsetzung des CRA, da hiervon Umfang und Tiefe der erforderlichen Compliance-Maßnahmen maßgeblich abhängen.

Verhältnis zu anderen Rechtsgrundlagen

Der CRA ergänzt bestehende Regelwerke wie die DSGVO, die NIS-2-Richtlinie oder die KI-Verordnung. Während die DSGVO den Schutz personenbezogener Daten und NIS-2 die Sicherheit der Organisation regeln, richtet sich der CRA unmittelbar auf die Sicherheit des Produkts selbst. Damit ist der CRA, wie die KI-Verordnung, dem Produkthaftungsrecht zuzuordnen.

Zur Erfüllung der CRA-Pflichten können zusätzliche Verarbeitungen personenbezogener Daten erforderlich werden, etwa für Schwachstellenmanagement, Protokollierung, Sicherheitsanalysen, Vorfallsmeldungen und die Bereitstellung von Sicherheitsupdates. Der CRA schafft hierfür jedoch keine eigenständige Rechtsgrundlage nach der DSGVO. Unternehmen müssen daher weiterhin geeignete datenschutzrechtliche Rechtsgrundlagen prüfen. Diese Rechtsgrundlagen können in der vertraglichen Durchführung, der gesetzlichen Verpflichtung oder gegebenenfalls im berechtigten Interesse bestehen.

Mehr Transparenz durch die Software Bill of Materials

Eine wesentliche Neuerung ist die für Hersteller verpflichtende Software Bill of Materials (SBOM bzw. Software-Stückliste). Sie dokumentiert sämtliche verwendeten Softwarekomponenten und schafft Transparenz über Lieferketten sowie mögliche Drittlandbezüge. Dadurch können Unternehmen, aber auch Aufsichtsbehörden und Betroffene Sicherheitsrisiken und den Transfer von Daten in Drittstaaten besser bewerten. Damit setzt der CRA einen Anreiz, ihre digitale Souveränität zu stärken.

Jetzt mit der Umsetzung beginnen

Auch wenn viele Anforderungen erst Ende 2027 vollständig gelten, sollten betroffene Unternehmen frühzeitig mit der Umsetzung beginnen. Die Analyse des Produktportfolios, die Einstufung nach den Risikoklassen des CRA, die Anpassung von Entwicklungsprozessen sowie die Überprüfung von Lieferanten und Verträgen benötigen erhebliche Vorlaufzeit.

Mithin ist zu beachten, dass sich die Themen Datenschutz, KI, Produkt- und Informationssicherheit künftig nicht mehr isoliert betrachten lassen. Damit setzt die Europäische Union den Trend fort, diese Rechtsgebiete enger miteinander zu verknüpfen. &

ALTHAMMER & KILL

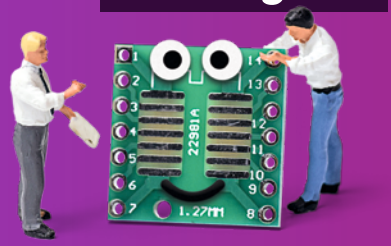
Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

Wir sind Digitalisierungskenner, Datenversteher und Vorwärtsdenker –
Ihr Experte für Datenschutz, Informationssicherheit, Künstliche Intelligenz und Compliance.
Unsere 45 Mitarbeitenden bringen Digitalisierung und Datenschutz bundesweit in Einklang.

Datenschutz

Informations-sicherheit

Künstliche Intelligenz



Compliance

althammer-kill.de

KLICK/SCAN