

Warum die ISO 42001 wichtig wird

friends of carmasec · 24. September 2026



Simon Decker

Senior Security Consultant · carmasec

Zwei Chatbots

Wer von beiden ist rechtlich der Hersteller?

GLOBEX.COM

Globex

Hallo! Wie kann ich helfen?

Chat powered by ChatPilot

Fertiges Produkt eingekauft

ACME.COM

ACME

Hi, ich bin Acki. Wie kann ich helfen?

ACME Industries

Von einer Agentur bauen lassen

ACME ist der Hersteller.

Im Gesetz heißt das Anbieter. Der Nutzer heißt Betreiber.



GLOBEX.COM

Globex

ANBIETER

ChatPilot, das Softwarehaus

BETREIBER

Globex

Die Agentur taucht nicht auf. Sie wäre Anbieter, wenn der Bot unter ihrem Namen lief.

ACME.COM

ACME

ANBIETER

ACME selbst

BETREIBER

ACME selbst

Anbieter ist, wer ein KI-System **entwickelt oder entwickeln lässt** und es **unter eigenem Namen** in Betrieb nimmt. Auch wenn es nur intern läuft.

Was an der Rolle hängt

Was in den Schilden steht, gilt ab 2. Dezember 2027 für Hochrisiko-Systeme.
Bei KI in regulierten Produkten ab 2. August 2028.

ANBIETER

verantwortet, wie es gebaut ist

Risiken über den Lebenszyklus steuern

Trainingsdaten prüfen und belegen

Technische Dokumentation erstellen

Aufsicht technisch ermöglichen

Genauigkeit und Robustheit sichern

Managementsystem führen

Markt beobachten, Vorfälle melden

BETREIBER

verantwortet, wie es eingesetzt wird

Einsetzen wie vorgesehen

Geeignete Leute an die Aufsicht

Passende Daten einspeisen

Betrieb überwachen, notfalls abschalten

Protokolle sechs Monate sichern

Beschäftigte und Betroffene informieren

2. Dezember 2026

Dann endet die Schonfrist für Bestandssysteme.

Systeme, die Texte, Bilder oder Audio erzeugen, brauchen eine maschinenlesbare Kennzeichnung. Für alles, was neu an den Start geht, gilt das **seit dem 2. August**. Was vorher schon lief, hat Schonfrist bis zum 2. Dezember.

Die Frist trifft Anbieter. Nicht Betreiber.

02.12.2027

Hochrisiko-Systeme

02.08.2028

KI in regulierten Produkten

6 bis 12 Monate

Aufbau eines Managementsystems



Die Verordnung verlangt ein Managementsystem.

Sie sagt nur nicht, welches.

Dort steht kein technisches Detail. Dort steht, wie ihr euch organisieren müsst.

Steht im Pflichtenkatalog für Anbieter, EU AI Act

Verlangt wird

Risikomanagement

Umgang mit Daten

Beobachtung nach Markteintritt

Meldung von Vorfällen

Dokumentation

Klare Verantwortlichkeiten

Und das ist die ISO 42001

Ein Zertifikat ist kein Freibrief. Aber ihr könnt die Frage beantworten, gegenüber Behörde und Kunde.

Heute zertifizierbar

Die einzige Norm für KI-
Managementsysteme, nach der ihr
euch schon jetzt zertifizieren lassen
könnt.

Zum Beispiel über den TÜV.

Beantwortet die Frage

Verzeichnis aller KI-Systeme, Rolle je
System, Risiko je System, wer
verantwortlich ist.

Dokumentiert und nachvollziehbar.

27001 zählt

Rahmen ist ähnlich. Neu sind die 38
KI-Controls im Anhang.

Rund die Hälfte davon steckt schon
in Iso 27001 zertifiziertem ISMS.

Drei Fragen für morgen früh

Nehmt euer auffälligstes KI-System. Dauert fünf Minuten.

- 1 Habt ihr es entwickelt oder entwickeln lassen?

- 2 Läuft es unter eurem Namen oder eurer Marke?

- 3 Erzeugt es Texte, Bilder oder Audio, und lief es schon vor dem 2. August 2026?

Zweimal ja, dann seid ihr vermutlich **Anbieter**.

Dreimal ja, dann ist eure Frist der **2. Dezember 2026**.

Seid ihr Anbieter oder Betreiber?

Der Unterschied ist nur, ob ihr die Frage stellt, bevor sie euch jemand anders stellt.

DREI GRÜNDE

- 1 Die Verordnung verlangt ein Managementsystem, und es gibt nur eine zertifizierbare Norm dafür
- 2 Die Vorlaufzeit macht aus Dezember 2027 einen Termin für dieses Jahr
- 3 Sie zwingt euch, die Frage vom Anfang zu beantworten

Lust auf Kontakt?



Simon Decker

simon.decker@carmasec.com

carmasec GmbH & Co. KG

