



Fabasoft Xpublisher

Datensicherheit trifft KI: Wie Xpublisher als cloud-natives Redaktionssystem neue Maßstäbe setzt

## Strafgerichtshof: Microsoft als Weckruf für digitale Souveränität

Microsoft hat nach Trump-Sanktionen den Internationalen Gerichtshof blockiert. Die Entscheidung ist ein Warnsignal für digitale Alternativen."



Der internationale Strafgerichtshof in Den Haag. (Bild: ICC)

## Business Punk

16. Juni 2025

# Meta schaltet Playboy Deutschland auf Facebook Verlag spricht von Angriff auf die Pressefreiheit

Autor\*in

Business Punk

Meta hat die offizielle Facebook-Seite des deutschen Playboy-Verlags nach einer Vorankündigung deaktiviert. Mehr als 1,9 Millionen Follower sind über eine Woche hinweg nicht erreichbar. Weder die Verlegerin Kouneli Metzger hinter der deutschen Ausgabe des Männermagazins noch die juristische Vertretung erhielten bisher eine offizielle Begründung von Meta.

Wirtschaft > Künstliche Intelligenz > KI und Urheberrecht: Anthropic darf Claude mit gekauften Büchern trainieren

## Künstliche Intelligenz Erfolg für KI-Konzern im Urheberrechtsstreit

25. Juni 2025, 16:10 Uhr | Lesezeit: 3 Min. | [Kommentare](#)



Ein US-Gericht hat entschieden, dass das Trainieren von KI-Modellen mit gekauften Büchern legal ist, obwohl Anthropic dabei gegen Urheberrechte verstoßen hat. (Foto: Dado Ruvic/REUTERS)

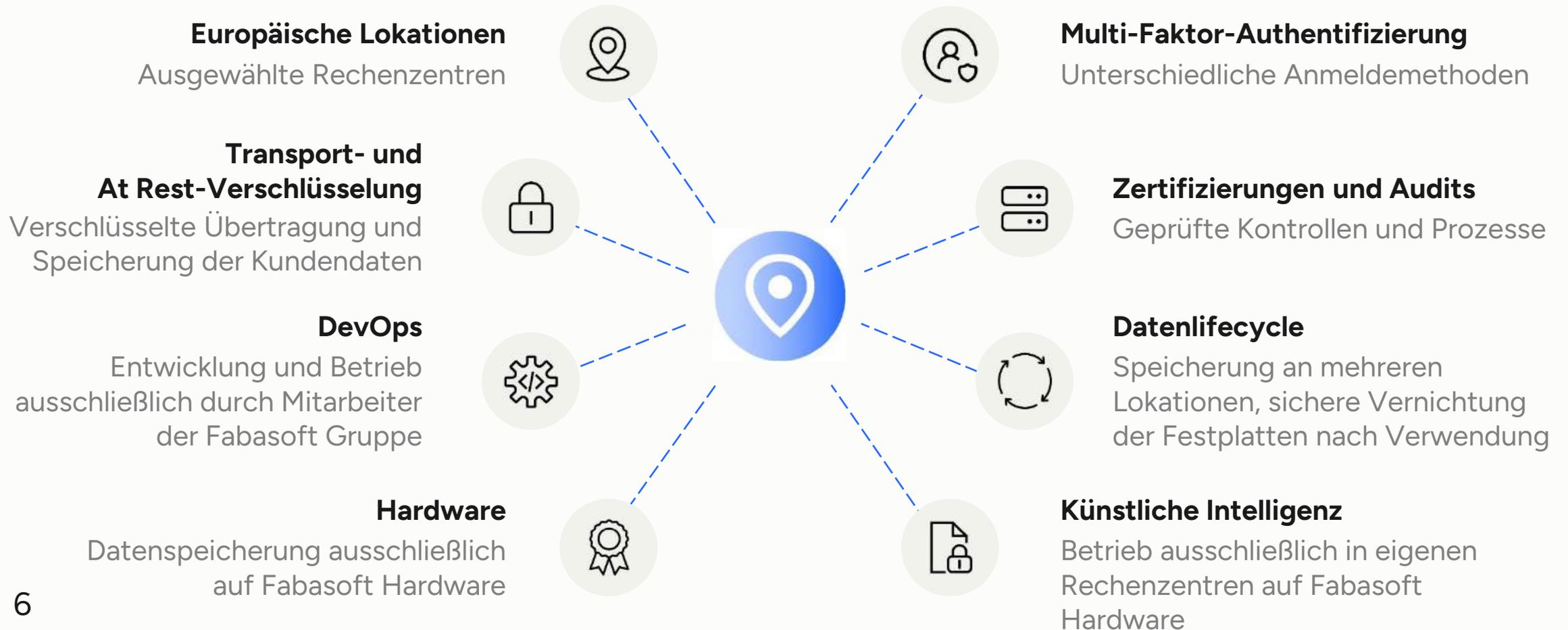
**Anthropic kaufte Millionen gedruckte Bücher, um seine KI-Modelle zu trainieren. Das war legal, sagt ein US-Richter. Trotzdem könnte es für das Unternehmen teuer werden.**

Wollen wir unsere Daten  
tatsächlich in die Hände von  
5 US Konzernen legen?

Künstliche Intelligenz wird  
die Verlagswelt verändern.

Wie können wir für eine  
maximale Datensicherheit  
und verlässliche Datenhoheit  
sorgen?

# Datensicherheit auf allen Ebenen



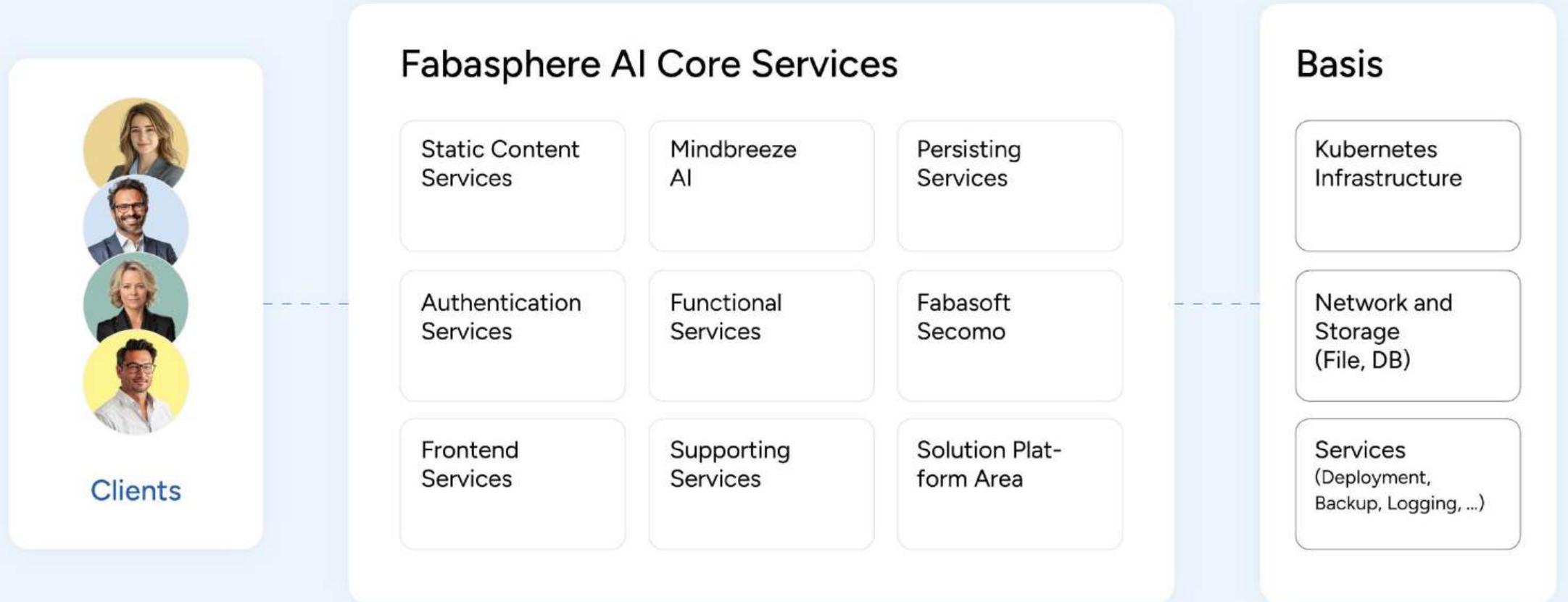
Der Begriff „cloud-native“  
beschreibt Software, die von  
Grund auf für die Cloud  
entwickelt wurde.

## Vergleich Cloud- und Betriebsmodelle

# Public vs. Private vs. On-Premises

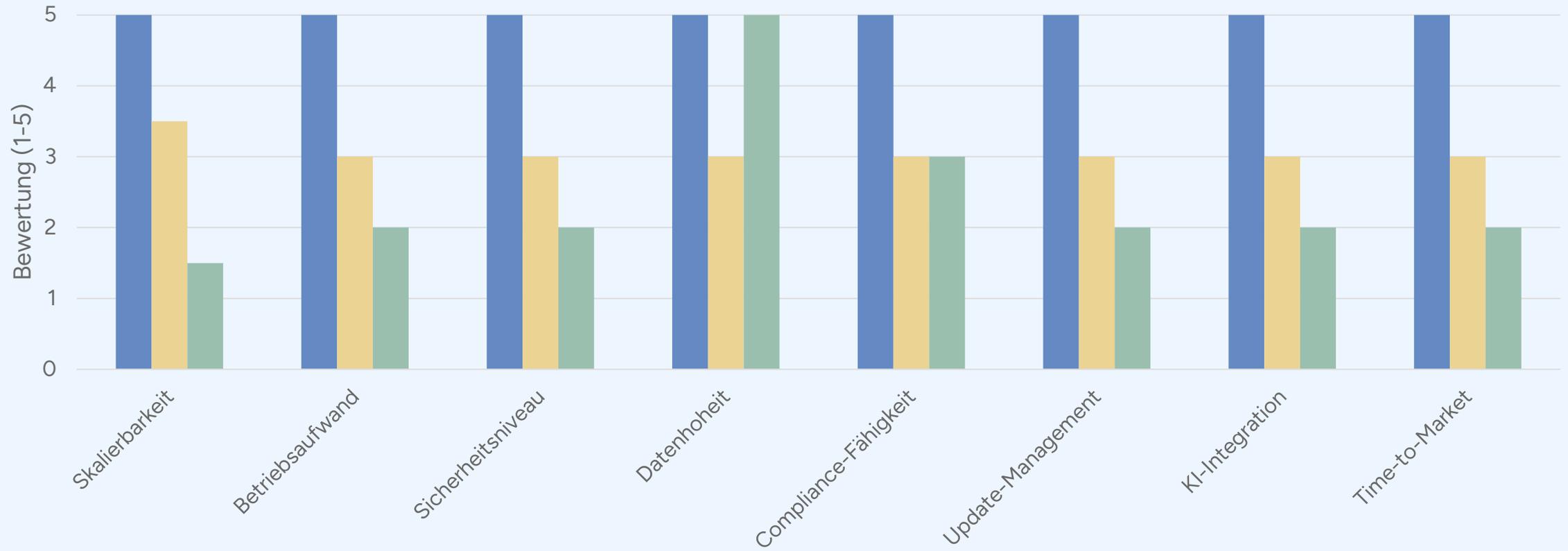
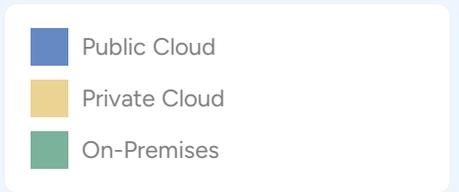
Kriterium	 <b>Public Cloud</b>	 <b>Private Cloud</b>	 <b>On-Premises</b>
Skalierbarkeit	Nahezu unbegrenzt, sofort verfügbar	Begrenzt skalierbar, abhängig von Ressourcen	Hardwaregebunden, schwer skalierbar
Betriebsaufwand	Minimiert – Provider übernimmt Betrieb	Interner Betrieb oder gehostet – teils hoher Aufwand	Vollständige Eigenverantwortung
Sicherheitsniveau	Höchste Sicherheitsstandards + Zertifizierungen	Gut – je nach Konfiguration und Budget	Volle Kontrolle – aber Ressourcenabhängig
Datenhoheit	Vollständig in Kundenhand (Datenregion, Verschlüsselung)	Teilweise – abhängig von Hostler und Architektur	Komplett – physische Kontrolle über Systeme
Compliance-Fähigkeit	Erfüllt regulatorische Vorgaben (z. B. BSI C5, SOC2, DSGVO)	Kann angepasst werden – aber oft mit Mehraufwand	Anpassbar, aber oft hoher Audit- und Adminalaufwand
Update-Management	Nahtlose Updates ohne Wartungsfenster	Updates manuell oder mit Wartungsfenster	Updates oft manuell mit Downtime
KI-Integration	Integrierte, selbst gehostete KI ohne Datenabfluss	KI meist extern angebunden oder limitiert	Kaum integrierte KI – meist Drittlösungen
Time-to-Market	Schnelle Bereitstellung & Innovation	Verzögert durch Individualisierung	Langsame Time-to-Market

# Cloud-native Building Blocks



## Vergleich Cloud- und Betriebsmodelle

# Public vs. Private vs. On-Premises



Vertrauen ist gut.  
Zertifizierte Sicherheit ist  
besser.

# Zertifizierte Zuverlässigkeit

Zertifizierungen und Audits:



Garantierte  
Verfügbarkeit (SLA)

99,9%

Zertifizierungen und Audits:



# Sicherheitsnachweis für ihre Daten durch BSI C5

„BSI C5 steht für "Cloud Computing Compliance Criteria Catalogue" und ist ein Kriterienkatalog des deutschen **Bundesamts für Sicherheit in der Informationstechnik** (BSI). Er definiert Mindestanforderungen an die Informationssicherheit von Cloud-Diensten, um eine transparente und sichere Nutzung von Cloud-Lösungen zu gewährleisten.“

- Belegt die Cloud-Sicherheit über Quellcode bis hin zu Betrieb
- Beobachtungszeitraum statt punktuelle Prüfung
- Testat wird durch Wirtschaftsprüfer ausgestellt

Wie sieht das für KI-basierte  
Anwendungen aus?

## Was wir unter KI-Sicherheit verstehen:

1. Zuverlässigkeit
2. Nachvollziehbarkeit
3. Verantwortlichkeit
4. Datensicherheit
5. Compliance

## Was wir unter KI-Sicherheit verstehen:

1. **Zuverlässigkeit**
2. Nachvollziehbarkeit
3. Verantwortlichkeit
4. Datensicherheit
5. Compliance

## Kriterienkatalog für KI-Cloud-Dienste – AIC4

Der Kriterien-Katalog [AIC4](#) (Artificial Intelligence Cloud Service Compliance Criteria Catalogue) spezifiziert Mindestanforderungen an die sichere Verwendung von Methoden des maschinellen Lernens in Cloud-Diensten. Er ist als Erweiterung des Kriterien-Kataloges [C5](#) (Cloud Computing Compliance Criteria Catalogue) konzipiert. Ziel ist die transparente Darstellung der Informationssicherheit eines KI-Cloud-Dienstes auf Basis einer standardisierten Prüfung. Diese kann von Cloud-Kunden im Rahmen einer eigenen Risikoanalyse verwendet werden. Der Kriterienkatalog [AIC4](#) wird von Cloud-Anbietern, Auditoren und Cloud-Kunden verwendet. Jede dieser Parteien hat eine Mitwirkungspflicht hinsichtlich der Informationssicherheit.

Der [C5](#) formuliert allgemeine Mindestanforderungen an sicheres Cloud Computing, welche für jeden Cloud-Dienst relevant sind. Der [AIC4](#) hingegen ergänzt spezielle Kriterien, die zusätzlich relevant sind, falls Methoden des maschinellen Lernens verwendet werden. Die Kriterien im [AIC4](#) adressieren die Bereiche Sicherheit und Robustheit, Performance und Funktionalität, Zuverlässigkeit, Datenqualität, Datenmanagement, Erklärbarkeit sowie Bias. Sie decken hierbei den gesamten Lebenszyklus von KI-Diensten ab, d. h. die Entwicklung, die Erprobung, die Validierung und den Betrieb.

[↓ AI Cloud Service Compliance Criteria Catalogue \(AIC4\)](#)

**Hinweis:** Der AIC4 ist nur in englischer Sprache verfügbar (vgl. FAQ zu Weiterentwicklung).

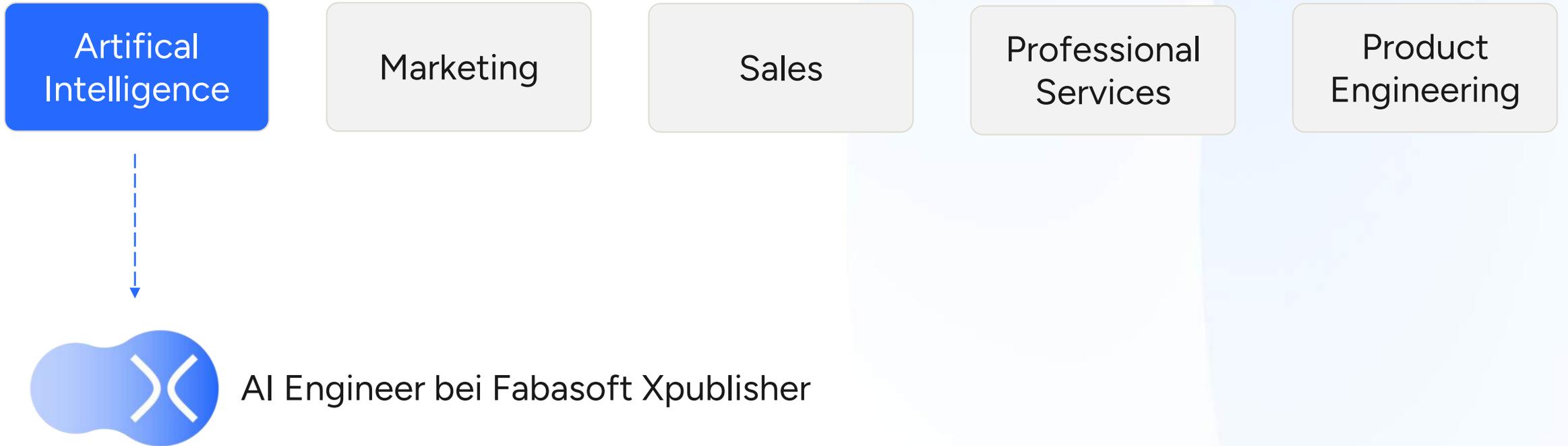
# Vertrauensnachweis für Künstliche Intelligenz durch BSI AIC4 (in Umsetzung)

„Der AIC4-Kriterienkatalog (Artificial Intelligence Cloud Services Compliance Criteria Catalogue) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist der weltweit einzig anerkannte, relevante Sicherheitsstandard für KI-basierte Anwendungen.“

- Belegt die Sicherheit im Umgang mit KI
- Basiert auf BSI C5 und ist eine inhaltliche Erweiterung
- Testat wird durch Wirtschaftsprüfer ausgestellt

Zuverlässigkeit der Ergebnisse

# KI-Kompetenz in der Fabasoft Gruppe



## SCRUM STORIES, RÜCKVERFOLGBARKEIT & AUDITS

- Schreiben von AI Features und AI Stories inklusive Formular
- Klar dokumentierte und kommunizierte Erwartungen an das AI Service
- Notwendige Kontrollen

Dokumentation

## USE-CASES MIT SOLUTION-/BASIS-CODE

- Verwendung von AI Komponenten
- UI Entwicklung
- Datenverwaltung
- Testautomatisierung mit Testplan

Programmierung

## MINDBREEZE AI IN FABASOFT CLOUD

- Entwicklung der KI-Modelle
- Prompt Engineering & Hyperparameter Tuning
- Test KI-Modell mit Mindbreeze AI in Fabasoft Cloud Evaluierungs-Framework

Künstliche Intelligenz

## SECURITY, NETZWERK UND DEPLOYMENT

- Konfiguration von Netzwerk- und Rechteinstellungen
- Rollenvergabe
- Notwendige Deployment von Mindbreeze AI in der Fabasoft Cloud
- Test im Live-Betrieb

Deployment



Zuverlässigkeit der Ergebnisse

# Leitfragen zur Vermeidung von Halluzinationen

- Identifizieren Sie kritische Geschäftsprozesse, die sich auf KI-Outputs stützen?
- Wird sich der Benutzer fälschlicherweise auf den Output verlassen?
- Bewerten Sie die potenziellen Auswirkungen von KI-Fehlern auf diese Prozesse?
- Erwägen Sie Fail-Safe-Mechanismen oder Human-in-the-Loop-Ansätze für Entscheidungen?
- Kann ein Benutzer den Output der KI modifizieren? Wie und warum?

## Was wir unter KI-Sicherheit verstehen:

1. Zuverlässigkeit
- 2. Nachvollziehbarkeit**
3. Verantwortlichkeit
4. Datensicherheit
5. Compliance

## Inhaltsübersicht

Kapitel I: Allgemeine Bestimmungen +

Kapitel II: Verbotene AI-Praktiken +

Kapitel III: Hochriskantes KI-System +

Kapitel IV: **Transparenzpflichtungen für Anbieter und Betreiber von bestimmten KI-Systemen** -

| [Artikel 50: Transparenzpflichtungen für Anbieter und Betreiber von bestimmten KI-Systemen](#)

Kapitel V: KI-Modelle für allgemeine Zwecke +

Kapitel VI: Maßnahmen zur Unterstützung der Innovation +

Kapitel VII: Governance +

Kapitel VIII: EU-Datenbank für hochriskante KI-Systeme +

Kapitel IX: Überwachung nach dem Inverkehrbringen, Informationsaustausch und Marktaufsicht +

 URL kopieren

Teil von [Kapitel IV: Transparenzpflichtungen für Anbieter und Betreiber bestimmter KI-Systeme](#)

# Artikel 50: Transparenzpflichtungen für Anbieter und Betreiber von bestimmten KI-Systemen

Datum des Inkrafttretens: **2. August 2026** Laut: **Artikel 113**

Einen vollständigen Zeitplan für die Umsetzung finden Sie [hier](#).

## ZUSAMMENFASSUNG +

**HINWEIS:** Diese Übersetzung ist eine maschinell erstellte Übersetzung. Es handelt sich nicht um die offizielle Übersetzung des Europäischen Parlaments, die Sie [hier finden](#) können.

1. (1) Die Anbieter stellen sicher, dass KI-Systeme, die für eine direkte Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen darüber informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus der Sicht einer natürlichen Person, die unter Berücksichtigung der Umstände und des Nutzungskontexts angemessen informiert, aufmerksam und umsichtig ist, offensichtlich. Diese Verpflichtung gilt nicht für KI-Systeme, die gesetzlich zur Aufdeckung, Verhütung, Untersuchung oder Verfolgung von

# Transparenz & Sichtbarmachung

- In Xpublisher ist die Interaktion bzw. der Einsatz von KI Features durch die User gekennzeichnet\*
- Zudem werden durch Mindbreeze AI erzeugte Inhalte gekennzeichnet (Metadaten)

Bild  
psrloDbaZc8

- Bearbeiten
- Herunterladen
- Hochladen
- Drehen
- Vorschlagworten



Teaser-Text ●

Kopieren

*Von der AI generierte Inhalte können ungenau oder fehlerhaft sein.*

Lieferketten stehen heute größeren Anforderungen denn je gegenüber. Besonders im projektbezogenen Maschinenbau, wo maßgeschneiderte Lösungen für den Kunden entwickelt werden, ist ein reibungsloses Zusammenspiel aller Beteiligten entscheidend.

Technische Dokumente wie Maßzeichnungen, 3D-Modelle, Qualitätszeugnisse, etc. müssen fristgerecht von den Zulieferern der jeweiligen Komponenten eingefordert sowie durch unterschiedliche Fachabteilungen geprüft und freigegeben werden.

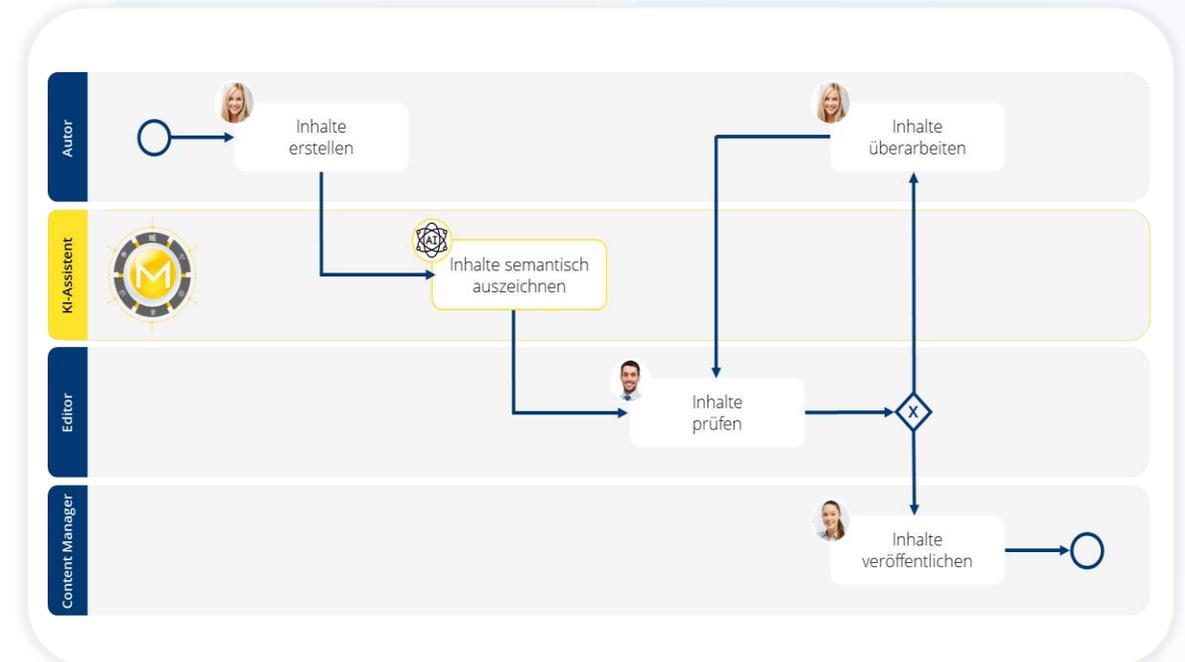
Solche Großprojekte zu managen und dabei sicherzustellen, dass jeder Beteiligte über einen einheitlichen Informationsstand verfügt und Fristen eingehalten werden, ist sehr zeitintensiv.

## Was wir unter KI-Sicherheit verstehen:

1. Zuverlässigkeit
2. Nachvollziehbarkeit
3. **Verantwortlichkeit**
4. Datensicherheit
5. Compliance

# Reduzierung von Haftungsrisiken

Falschinformationen stellen ein großes Risiko in der redaktionellen Arbeit dar, insbesondere wenn KI-generierte Inhalte ohne ausreichende Prüfung veröffentlicht werden. Um Haftungsrisiken zu minimieren, empfehlen sich **hybride Workflows**.



KI ↔ Mensch Mensch



**HUMAN**

in the loop

## Was wir unter KI-Sicherheit verstehen:

1. Zuverlässigkeit
2. Nachvollziehbarkeit
3. Verantwortlichkeit
4. **Datensicherheit**
5. Compliance

# Verlassen Sie sich auf höchste Datensicherheit

Mindbreeze AI bündelt verschiedene **KI-Technologien in eigenen Rechenzentren.**

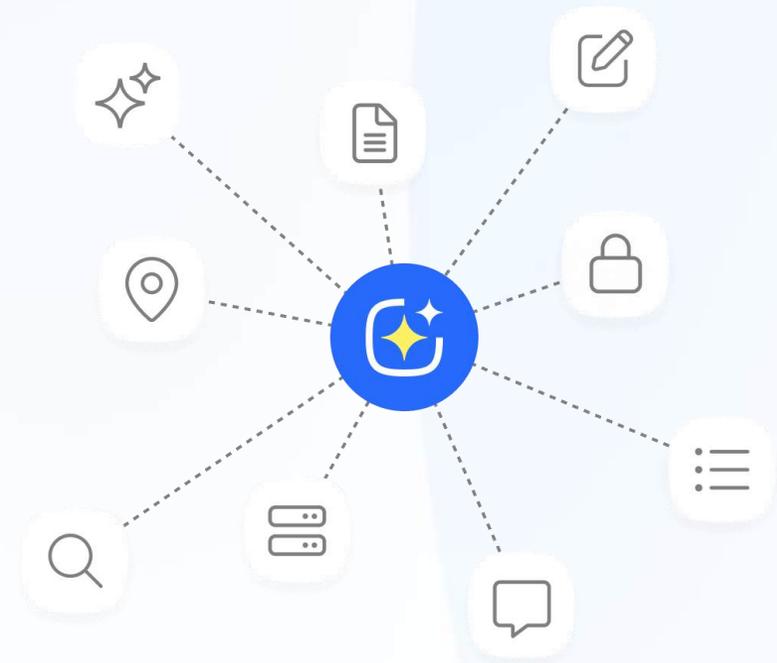


Datenschutz & Isolation: Jeder Kunde nutzt eine eigene Mindbreeze Instanz, **Daten bleiben dabei geschützt.**



# Vorteile durch den Einsatz vortrainierter, durch uns betriebener LLMs

- Vortrainierte Sprachmodelle greifen auf eine bereits erlernte, leistungsstarke Basis zurück.
- Dies reduziert den Trainingsaufwand sowie die IT-Kosten erheblich.
- Zudem kann in kurzer Zeit ein hohes Qualitätslevel erreicht werden.



## Was wir unter KI-Sicherheit verstehen:

1. Zuverlässigkeit
2. Nachvollziehbarkeit
3. Verantwortlichkeit
4. Datensicherheit
5. **Compliance**

# Mögliche Bausteine einer KI-Compliance-Richtlinie

## 1 Bewertung & Auswahl von KI-Systemen

## 2 Aufstellen eines KI-Regelwerkes

Durchführung von Nutzertrainings

(Gegen-) Prüfung der Ergebnisse

Interne Kennzeichnungspflichten KI-generierter Inhalte

## 3 Durchführung von Nutzertrainings

## 4 Aufbau von Experten-Wissen, Know-How-Transfer

## 5 Permanente Risiko-Bewertung

Ready for  
**EU AI ACT**

# Mit Fabasoft Xpublisher mögliche Rechtsrisiken vermeiden

## 1 Datensicherheit

Gewährleistung eines den jeweiligen Daten entsprechenden Schutzniveaus.

## 2 AI Literarcy

Pflicht, ein ausreichendes Maß an KI-Kompetenz innerhalb des Unternehmens sicherzustellen.

## 3 Verbotene KI

Stark subliminale Techniken, also das Einbinden unterschwelliger manipulativer Botschaften/Signale.

## 4 Fehlinformationen

Haftung für falschen Output der KI, der durch ein Unternehmen veröffentlicht wird.

## 5 Transparenz

Kennzeichnungspflicht von KI-generierten Inhalten und dem Einsatz von KI-Technologie.

## 6 Urheberrecht

Bedingter Schutz eigener Inhalte gegen KI-Training und KI-basierte Inhalte gegen Drittverwendung.

# Unser Softwareangebot

# Xpublisher

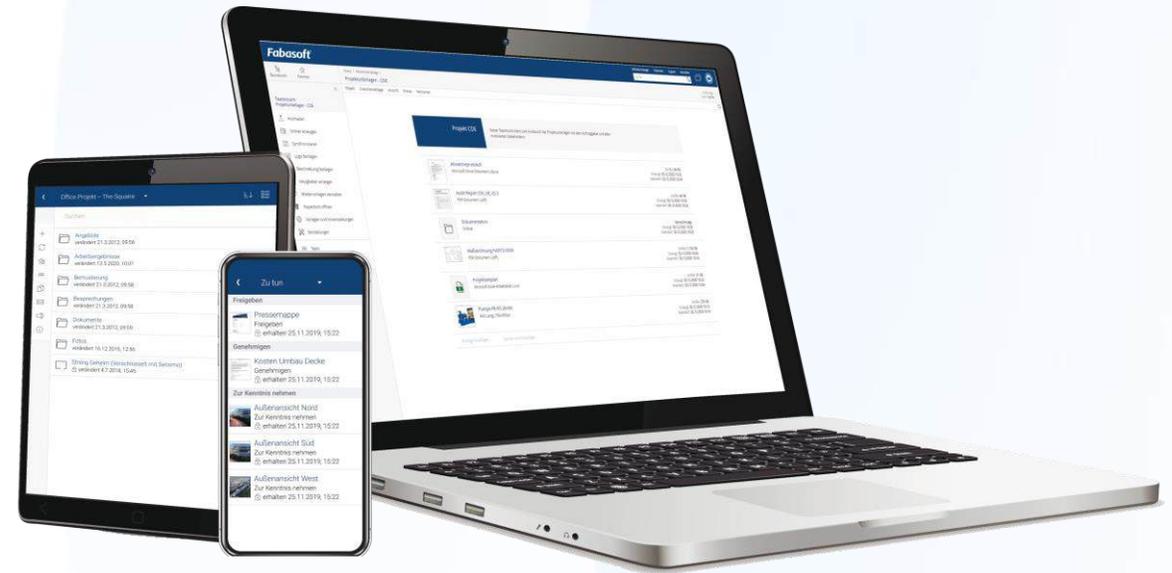
ist ein workflowzentriertes Redaktions- und Publishingsystem mit dem unterschiedliche Inhalte erstellt, in einem Contentpool verwaltet und hocheffizient publiziert werden können.

**DIGITAL und PRINT**



# Arbeiten Sie wann und wo Sie wollen

- Cloudbasierte Lösung mit sicherer 2-Faktor-Authentifizierung und Single-Sign-on
- Ortsunabhängiges Arbeiten durch responsive Web-Interface
- Schnelles Erledigen von Aufgaben durch optimierte mobile Apps für iOS und Android
- Oberfläche in über 20 verschiedene Sprachen übersetzt und barrierefrei nutzbar
- Unlimitierte Anwendungen und Skalierbarkeit: Benutzer und Speicher jederzeit erweiterbar



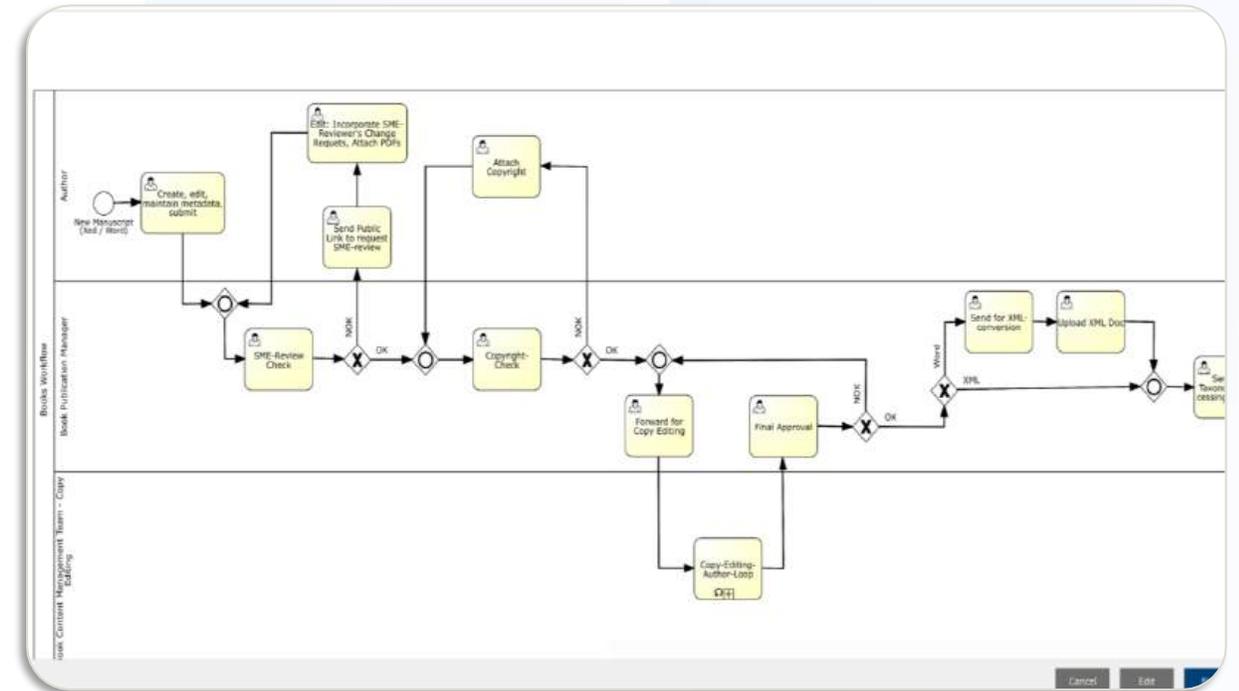
~~Print first~~

~~Digital first~~

Content first

# Digitalisierung der Prozesse für mehr Effizienz

- Modellieren Sie Ihre individuellen Workflows mit dem integrierten BPMN-Workflow-Editor
- Automatisierung Sie Arbeitsabläufe inkl. Fristen & Verantwortlichkeiten
- Workflows nach Taskforce-IT-Standards bereits umgesetzt



Mindbreeze  
AI

Fabasoftware Ecosystem

## AI Use Cases

Intelligent Document  
Processing (IDP)

---

Prozesssteuerung  
mit Agentic AI

---

Dialog mit Dokumenten

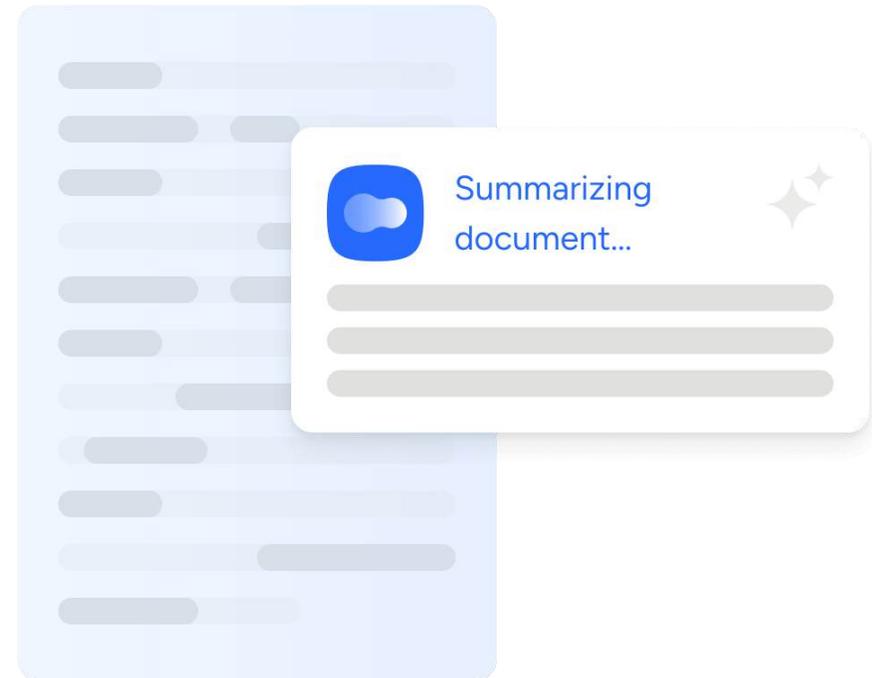
---

Proaktives  
Informationsmanagement

# Generative KI als Redaktionsassistent



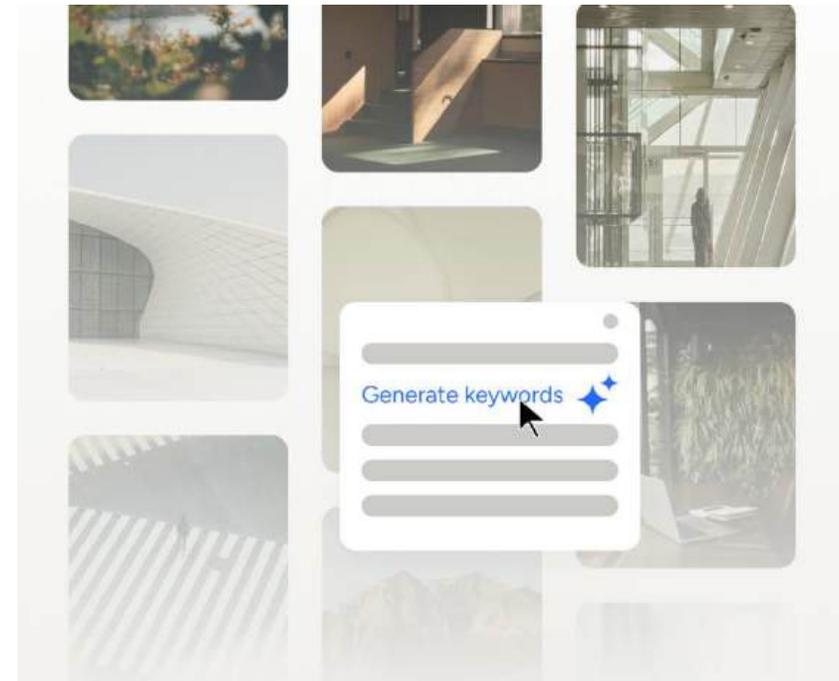
Mit den von Mindbreeze AI zur Verfügung gestellten LLMs (Large Language Models) ermöglicht Xpublisher die effiziente Erstellung generativer Inhalte wie Zusammenfassungen, Teaser oder Social-Media-Posts.



# Verschlagworten Sie digitale Assets automatisch



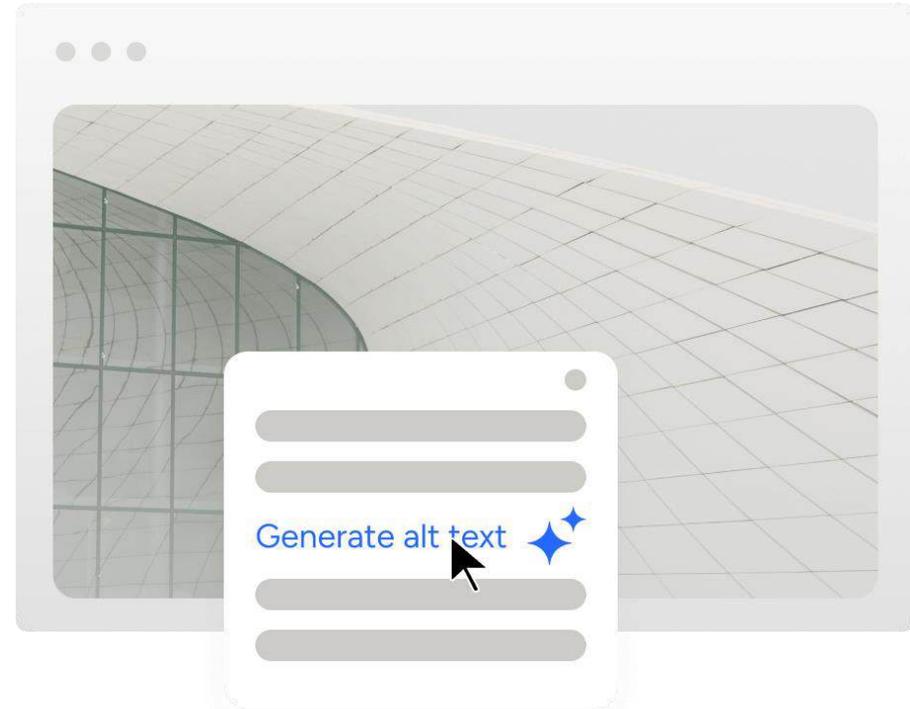
Die KI analysiert die digitalen Assets – Bilder, Videos und Dokumente –, erkennt relevante Elemente wie Personen, Objekte, Orte oder Themen und leitet daraus Schlagwörter ab.



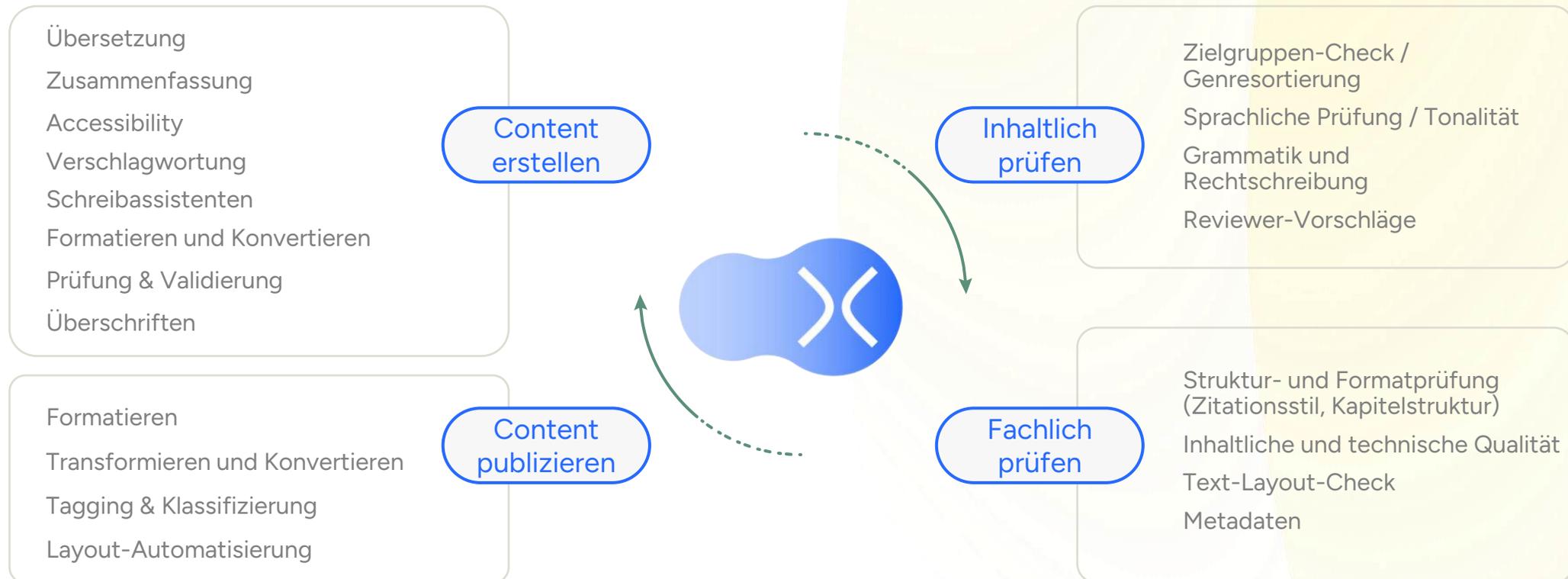
# Erhöhen Sie durch automatisierte Alt-Texte die Barrierefreiheit



Die integrierte KI generiert automatisch präzise Alternativtexte (Alt-Texte) für Bilder. Diese sind einerseits für die Einhaltung des Barrierefreiheitsstärkungsgesetzes unerlässlich, andererseits auch ein wichtiger Bestandteil der Suchmaschinenoptimierung (SEO)



# KI-Use Cases in Redaktion und Lektorat



**Vielen Dank**



**Matthias Kraus**

Gründer und Head of Sales



+49 (0)89 5472617850



matthias.kraus@fabasoft.com



Jetzt QR Code scannen und  
**KI-Checkliste** herunterladen

## Disclaimer

**Copyright © Fabasoft Xpublisher GmbH, 80333 München, 2025.**

Alle Rechte vorbehalten. Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Marken der jeweiligen Hersteller.

Fabasoft übernimmt in diesem Dokument weder implizite noch explizite Verpflichtungen, insbesondere nicht dafür, dass das Dokument vollständig und fehlerfrei ist.

Diese Präsentation enthält Angaben, die sich auf die erwartete zukünftige Entwicklung beziehen. Diese zukunftsbezogenen Aussagen werden üblicherweise – jedoch nicht ausschließlich – mit Begriffen wie „erwarten“, „schätzen“, „planen“ usw. umschrieben. Zukunftsbezogene Aussagen erheben keinen Anspruch auf Richtigkeit und Vollständigkeit, werden nicht aktualisiert und sind daher mit der gebotenen Vorsicht zur Kenntnis zu nehmen. Diese Präsentation wurde mit größtmöglicher Sorgfalt erstellt und die angegebenen Daten überprüft. Rundungs-, Satz- und Druckfehler können aber dennoch nicht ausgeschlossen werden.

Fehler und Irrtümer vorbehalten.