

China reguliert KI-Agenten zuerst: Die Lehre für Schweizer KMU

MANAGEMENT SUMMARY & KERNAUSSAGE

China hat im Juli 2026 als erstes Land weltweit verbindliche Regeln speziell für KI-Agenten erlassen: ein Drei-Stufen-Autorisierungsmodell, Melde- und Rückrufpflichten für sensible Branchen sowie strikte Vorgaben für emotionale KI. Für Schweizer KMU mit China-Geschäft ist das sofort bindend – und ein Vorbote dessen, was in absehbarer Zeit auch in der EU und der Schweiz ankommen dürfte.

KONTEXT & RELEVANZ FÜR ENTSCHEIDER

Am 15. Juli 2026 sind in China zwei neue Regelwerke in Kraft getreten, die weltweit als erste verbindliche Vorschriften eigens für KI-Agenten gelten. Sie unterscheiden erstmals ausdrücklich zwischen autonomen Agenten – Systemen mit eigener Wahrnehmung, Gedächtnis, Entscheidungsfähigkeit, Interaktion und Handlungsvermögen – und gewöhnlichen generativen Chatbots. Für Schweizer Unternehmen mit Geschäft in oder mit China ist das ab sofort geltendes Recht. Für alle anderen ist es die deutlichste Vorschau darauf, wie Regulierer weltweit – auch in Brüssel und Bern – autonome KI in den kommenden Monaten behandeln dürften.

In der öffentlichen Debatte kursiert die verkürzte Aussage, Chinas Agenten-Regelwerk sei am 15. Juli 2026 in Kraft getreten. Das stimmt nur zur Hälfte. Die Implementation Opinions on the Standardized Application and Innovative Development of Intelligent Agents wurden bereits am 8. Mai 2026 von der Cyberspace Administration of China, der staatlichen Entwicklungs- und Reformkommission sowie dem Industrieministerium erlassen. Es handelt sich um ein politisches Rahmenwerk, keine fertige Vollzugsverordnung – viele Standards, Filing-Mechanismen und Rückrufverfahren muss der Gesetzgeber erst noch ausarbeiten. Am 15. Juli trat stattdessen ein anderes, bereits bindendes Instrument in Kraft: die Interim Measures for the Administration of AI Anthropomorphic Interactive Services, die gezielt emotionale Companion-KI regulieren und Arbeits-Agenten bewusst aussparen.

KERN-HANDLUNGSEMPFEHLUNGEN

- 01 Stufe 1 – dem Menschen vorbehalten: Handlungen mit hoher Tragweite oder Irreversibilität, etwa Verträge, Zahlungen oder medizinische Entscheidungen
- 02 Stufe 2 – nur mit Nutzerautorisierung: Aktionen, die der Agent vorschlägt, aber erst nach expliziter Freigabe ausführt
- 03 Stufe 3 – autonom zulässig: Routineaufgaben mit geringem Risiko, die der Agent eigenständig ausführen darf

SCHWEIZER UMSETZUNGSKRITERIEN (REVDSG & IT-ARCHITEKTUR)

- ☑ Vollständige Konformität mit dem neuen Schweizer Datenschutzgesetz (revDSG).
- ☑ Keine Abhängigkeiten: Zero Lock-In auf proprietäre geschlossene Modelle.
- ☑ Schnittstellen zu Schweizer ERPs (Abacus, Bexio, M365) im operativen Betrieb.

Unverbindliche Prozess-Analyse

Lass uns in 20 Minuten prüfen, wo KI-Agenten in deinem Unternehmen sofort messbare Entlastung schaffen.

ki-outsourcing.ch