mmind.ai × bratschi

AI COMPLIANCE UMFRAGE 2026 · SCHWEIZ UND LIECHTENSTEIN

KI in der Compliance: was heute schon funktioniert.

32 Compliance-Verantwortliche haben uns gezeigt, wo ihre Zeit verloren geht. Dieses Papier sagt, welche dieser Aufgaben KI-Modelle 2026 übernehmen, welche nicht, und wie der erste Schritt aussieht.

MMIND.ai und Bratschi Rechtsanwälte
Umfrage März bis Mai 2026, n=32

Stand August 2026
Aktualisiert am 23. September 2026

INHALT

Was in diesem Papier steht.

Teil I bringt die Umfrage auf sechs Seiten. Teil II übersetzt sie in vier Aufgaben, an denen die Arbeitszeit hängt. Teil III zeigt, welche dieser Aufgaben heutige KI-Modelle übernehmen und welche nicht. Teil IV beschreibt den Weg zur ersten Umsetzung.

TEIL I · WAS DIE UMFRAGE ZEIGT

1 Sie brauchen kein Software-Projekt mehr 03

2 Die Lage in Zahlen 04

3 Unsere Stichprobe im Überblick 06

TEIL II · WO DIE ZEIT HÄNGT

4 Der grösste Hebel liegt beim Reporting 07

5 Ihre Daten sind PDFs, keine Datenbank 09

6 Der Wunsch nach intern kollidiert mit dem Markt 10

TEIL III · WAS KI-MODELLE DAVON LÖSEN

7 Chat, Ordner mit Ablauf, eigene Anwendung 11

8 Ihr Werkzeug kann das schon 12

9 Fallbeispiel A: Zertifizierungs-Navigator 14

10 Wann sich eine eigene Anwendung lohnt 16

11 Fallbeispiel B: Nachhaltigkeits-One-Pager 17

12 Entscheidend ist, wo Ihre Dokumente liegen 19

13 Risiken, die den Einsatz begrenzen 21

TEIL IV · WIE DER ANFANG AUSSIEHT

14 Erst optimieren, dann digitalisieren 22

15 Governance-Minimum vor dem ersten Ablauf 24

ANHANG

A Topline je Frage · B Quellen · C Codierung 25

01 · MANAGEMENT SUMMARY

Sie brauchen kein Software-Projekt mehr.

Erstens. Compliance-Arbeit ist heute zu einem grossen Teil Informationslogistik von Hand. 81 Prozent verfolgen Regulatorik über manuelle Recherche, 6 Prozent mit einem spezialisierten Werkzeug.

Zweitens. Der Aufwand dafür ist hoch. Jede zweite Organisation wendet 20 Stunden pro Woche oder mehr für manuelle Compliance-Aufgaben auf. Nur 13 Prozent bleiben unter fünf Stunden.

Drittens. 56 Prozent messen die Wirksamkeit ihres Programms nicht. Die Gründe sind technisch, nicht kulturell: 83 Prozent dieser Gruppe nennen eine fehlende Datenbasis, 61 Prozent kein geeignetes Werkzeug.

Viertens. Gesucht wird kein weiteres Dashboard. 75 Prozent wollen intern oder hybrid verarbeiten, 84 Prozent arbeiten mit unstrukturierten Dokumenten. Gefragt ist ein kontrollierter Prozess auf den eigenen Daten.

Fünftens. Genau dieser Prozess braucht seit 2026 kein Softwareprojekt mehr: ein definierter Ordner, ein hinterlegter Ablauf, ein nachvollziehbares Ergebnis. Wir zeigen zwei Umsetzungen und die Grenzen, die dabei nicht verhandelbar sind.

02 · VERDICHTUNG

Die Lage in Zahlen.

81%
verfolgen Regulatorik über **manuelle Recherche**
26 von 32

6%
nutzen dafür ein **spezialisiertes Tool**
2 von 32

50%
wenden **20 Stunden pro Woche oder mehr** für manuelle Arbeit auf
16 von 32

56%
messen die **Wirksamkeit nicht**
18 von 32

84%
arbeiten mit **unstrukturierten Dokumenten**
27 von 32

91%
nennen **Reporting** als Kernfunktion
29 von 32

75%
wollen **intern oder hybrid** verarbeiten
24 von 32

53%
fehlt **interne KI-Governance-Expertise**
17 von 32

Der Aufwand, um den es geht

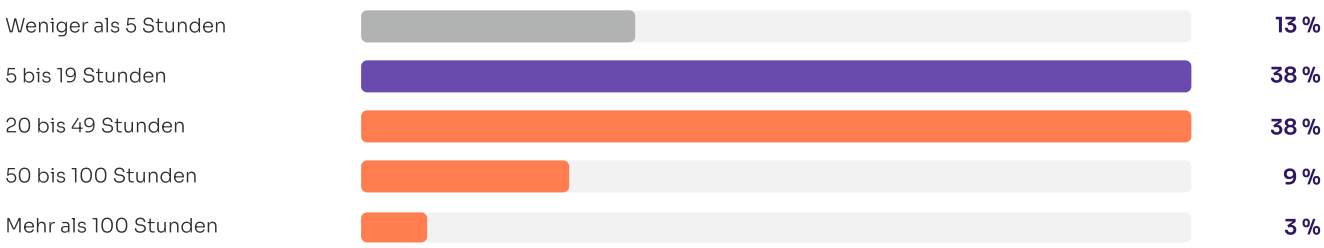


Abbildung 1: Zeitaufwand pro Woche für manuelle Compliance-Aufgaben (n=32). Orange markiert die 50 Prozent ab 20 Stunden, also 16 Organisationen. Bei n=32 entspricht eine Person rund 3 Prozentpunkten; wir nennen deshalb überall auch die absolute Zahl.

> Jede zweite Organisation arbeitet ein halbes Pensum pro Woche für Aufgaben ab, die kaum ein Urteil erfordern. Es geht um das Zusammentragen, Umformatieren und Weiterleiten von Information.

Wie Regulatorik heute verfolgt wird

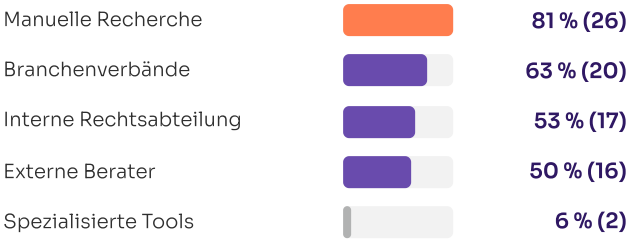


Abbildung 2: Mehrfachnennungen, n=32. 94 Prozent arbeiten heute ohne Regulatory-Intelligence-Werkzeug.

Welche Daten überhaupt vorliegen

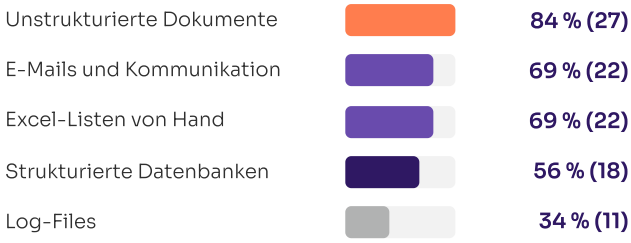


Abbildung 3: Mehrfachnennungen, n=32. Der Rohstoff ist Text. Das entscheidet über die Werkzeugklasse.

Die Lücke zwischen Anspruch und Nachweis

56 % messen die Wirksamkeit ihres Compliance-Programms **nicht regelmässig** (18 von 32).

Die 44 Prozent, die messen, tun es überwiegend operativ: Schulungsquoten, Fallzahlen, geprüfte Verträge. Nur wenige messen so, dass sich daraus eine Steuerungsentscheidung ableiten liesse. Für die Akzeptanz auf Geschäftsleitungsebene ist genau das der Engpass.

Warum nicht gemessen wird (Basis: die 18)

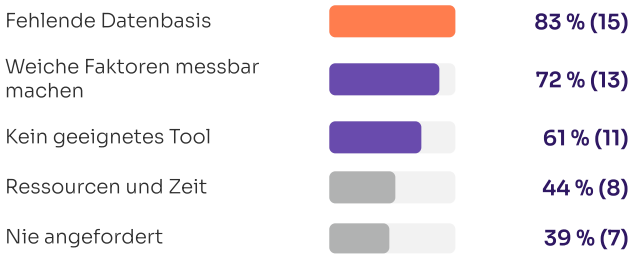


Abbildung 4: Zwei der drei häufigsten Gründe sind Werkzeug- und Datenprobleme, also lösbar.

03 · STICHPROBE

Unsere Stichprobe im Überblick.

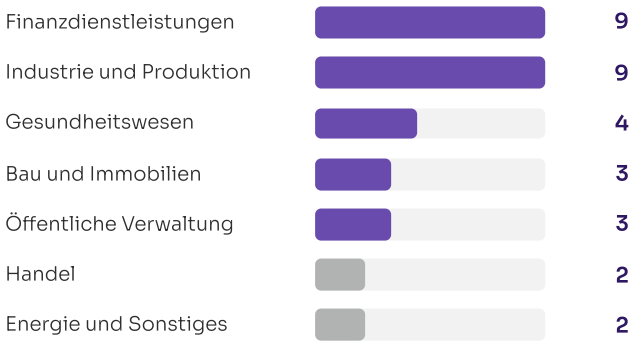
Grundlage ist eine Online-Befragung von 32 Compliance-Verantwortlichen mit Bezug zum Schweizer und liechtensteinischen Markt, erhoben zwischen dem 18. März und dem 31. Mai 2026.

32 ist für diesen Fragebogen eine gute Zahl. Erhoben wurden 35 Fragefelder, darunter offene Fragen zu Pain Points, Rechtsgebieten und Wunschfunktionen. Wer das ausfüllt, sitzt eine halbe Stunde daran. Genau das ist die Stärke dieser Daten: Alle 32 Einreichungen waren serverseitig valide, und im Schnitt blieben nur drei der 35 Felder leer, meist solche, die bei der jeweiligen Antwort ohnehin entfielen. Es sind keine schnell weggeklickten Panel-Antworten, sondern Auskünfte von Personen, die sich Zeit genommen haben. Die Freitexte zeigen das: «Bei Compliance-Filtern zu viele false positive Treffer, die manuell abgearbeitet werden müssen» schreibt niemand, der einen Fragebogen überfliegt.

Bei der Lesart sind wir streng. Mehrfachauswahlfragen berichten wir als Anzahl Nennungen und als Anteil der Befragten, nicht als Verteilung. Die Summe der Anteile übersteigt deshalb regelmässig 100 Prozent. Bei bedingten Fragen nennen wir die reduzierte Basis ausdrücklich, etwa «Basis: die 18, die nicht messen». Freitextantworten sind thematisch codiert; das Schema steht in Anhang C.

Zwei Punkte gehören offengelegt. Die Stichprobe ist eine gezielte Auswahl von Fachpersonen, keine Zufallsstichprobe der Grundgesamtheit. Und sie ist zu grossen Organisationen verschoben: 72 Prozent haben 300 oder mehr Mitarbeitende. Befunde zu Ressourcen und Governance-Reife dürften für KMU eher schlechter aussehen, nicht besser.

Branchenprofil



Organisationsgrösse

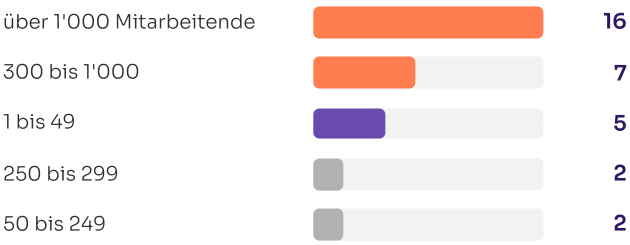


Abbildung 5: Stichprobenprofil (n=32). Finanzdienstleistungen und Industrie stellen je 28 Prozent. Der Schwerpunkt bei grossen Organisationen ist bei der Übertragung auf KMU mitzudenken.

04 · BEDARF

Der grösste Hebel liegt beim Reporting.

Reduziert man die 35 Fragefelder auf ihren gemeinsamen Kern, bleiben vier Aufgaben. Sie unterscheiden sich strukturell, und nur zwei davon lassen sich heute zuverlässig automatisieren. Darauf baut Teil III auf.

AUFGABE 1

Wissen, was sich geändert hat

Regulatorik verfolgen, filtern, auf die eigene Organisation beziehen. 81 Prozent tun das über manuelle Recherche, 63 Prozent über Verbände, 50 Prozent über externe Berater. 6 Prozent nutzen ein spezialisiertes Werkzeug. Aus dem Freitext: «Überflutung mit Informationen und Regeln», «Überblick zu den aktuellen Anforderungen auch in anderen Rechtsräumen».

Automatisierbar? Teilweise. Als Signalgeber mit Quellenpflicht, nie als Rechtsauskunft. Siehe Kapitel 13.

AUFGABE 2

Berichte und Nachweise erzeugen

Der häufigste Bedarf überhaupt. 91 Prozent nennen Reporting als Kernfunktion, 59 Prozent sehen Berichterstattung als am ehesten automatisierbare Tätigkeit. 72 Prozent nennen das jährliche Compliance-Risk-Assessment als automatisierbaren Prozess, den Spitzenwert aller dreizehn abgefragten Prozesse.

Automatisierbar? Ja, gut. Wiederkehrend, klar begrenzt, Ergebnis sofort prüfbar. Der beste Startpunkt.

AUFGABE 3

Wirksamkeit belegen können

56 Prozent messen nicht. In dieser Gruppe nennen 83 Prozent eine fehlende Datenbasis und 61 Prozent das fehlende Werkzeug, also technische Probleme. Bemerkenswert: 9 der 16 Organisationen mit 20 Stunden Aufwand und mehr pro Woche messen dennoch nicht. Es wird viel gearbeitet und wenig belegt.

Automatisierbar? Ja, sobald Block 2 läuft. Kennzahlen fallen als Nebenprodukt eines strukturierten Berichtsprozesses an.

AUFGABE 4

Die eigene KI regulieren

Für 94 Prozent ist KI-Regulierung ein Thema. 38 Prozent haben erste Abklärungen getroffen, je 28 Prozent beobachten oder haben Governance etabliert. Die grösste Hürde liegt bei den Menschen, nicht in der Technik: 53 Prozent nennen fehlende interne KI-Governance-Expertise, je 47 Prozent die Klassifizierung der eigenen Systeme und unklare regulatorische Anforderungen.

Automatisierbar? Nein. Das ist eine Kompetenz- und Entscheidungsfrage. Werkzeuge helfen erst danach.

Die bemerkenswerteste Zahl der Umfrage ist eine Kombination: sechs Organisationen haben KI-Governance etabliert und nennen gleichzeitig fehlende interne Expertise als Hürde. Governance auf Papier ist noch keine Kompetenz in der Linie.

Welche Prozesse konkret automatisiert werden sollen

Frage 11, Mehrfachnennungen, n=32. Im Median nennt jede Person fünf Prozesse. Der Bedarf ist breit, nicht punktuell. Die vier obersten Positionen gehören zu Aufgabe 1 und 2.

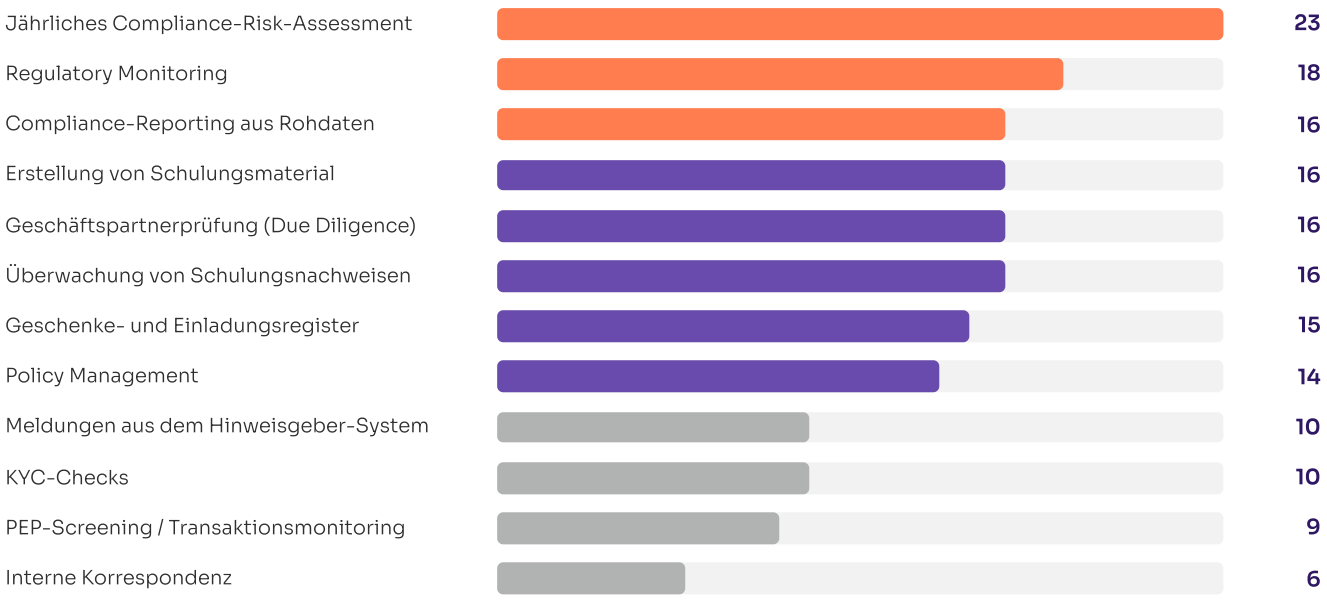
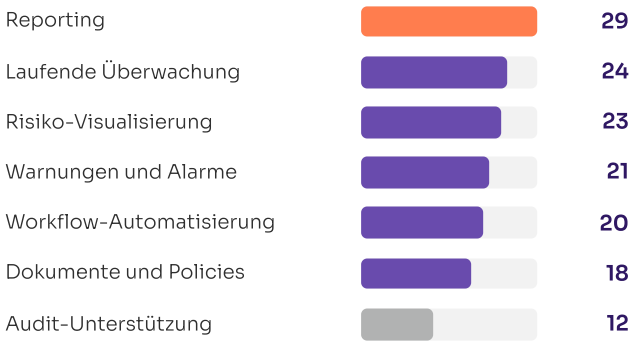


Abbildung 6: Automatisierungswünsche nach Prozess. Orange markiert die drei Prozesse, die hohe manuelle Last mit klar begrenzten, wiederholbaren Schritten verbinden und sich deshalb als Erstes eignen.

Was ein Cockpit können soll



Wann gewarnt werden soll

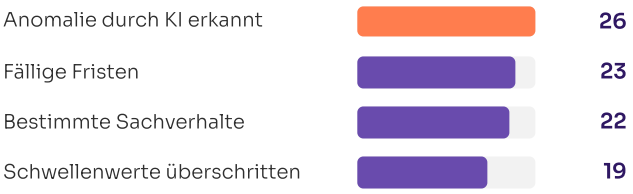


Abbildung 7: Der häufigste Auslösewunsch ist ausgerechnet der anspruchsvollste: KI-erkannte Anomalien. Fristen und Sachverhalte sind deterministisch und deshalb der ehrlichere Anfang.

05 · DATENLAGE

Ihre Daten sind PDFs, keine Datenbank.

Diese eine Zahl entscheidet über die Werkzeugklasse: 27 von 32 nennen unstrukturierte Dokumente als wichtigste Datenquelle, also PDF-Verträge, Word-Richtlinien, Weisungen und Protokolle. Danach kommen E-Mails und von Hand gepflegte Excel-Listen mit je 22 Nennungen. Strukturierte Datenbanken liegen mit 18 Nennungen dahinter.

22 von 32 verbinden beides: manuelle Recherche und unstrukturierte Dokumente als Hauptquelle. So sieht die Arbeitsrealität aus: Menschen lesen Text und schreiben Zusammenfassungen.

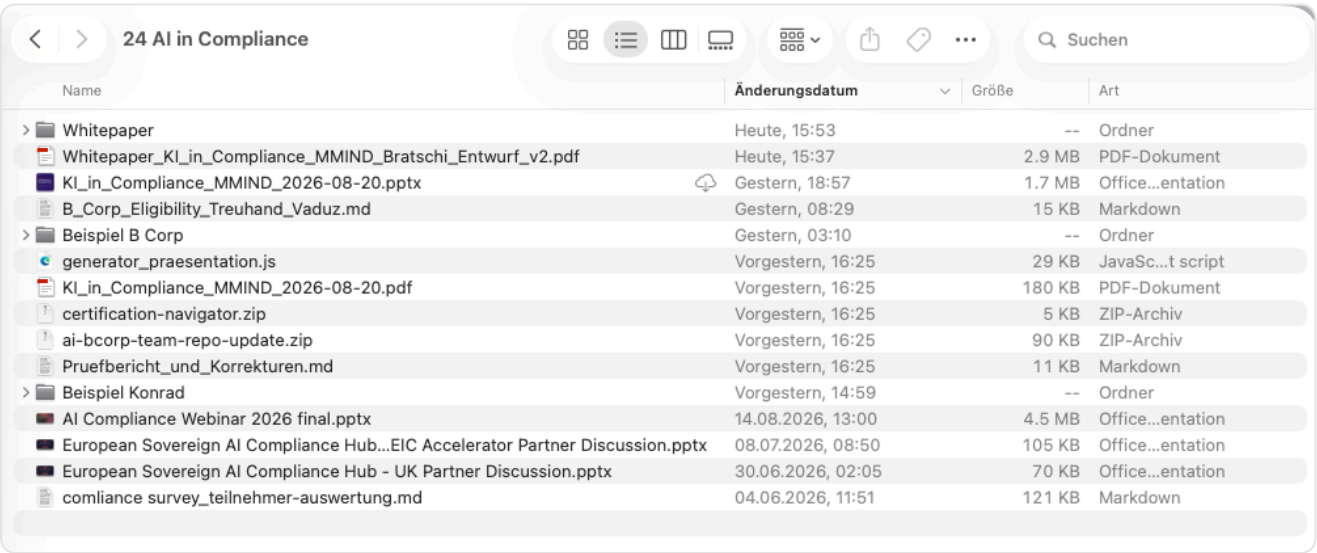
Klassische GRC- und Business-Intelligence-Werkzeuge setzen an der Tabelle an. Sie erwarten Felder, Schwellenwerte und Schnittstellen. Genau dort liegt der Bedarf aber nicht. Ein Werkzeug, das Text liest, Belegstellen zitiert und daraus eine Tabelle erst erzeugt, passt zur Datenlage. Eines, das eine gepflegte Datenbank voraussetzt, verschiebt die Arbeit nur nach vorn.

Das erklärt auch, warum 15 von 32 eine vollautomatische API-Anbindung in Echtzeit wünschen, während gleichzeitig 5 mit «Ich weiss es nicht» antworten: Der Wunsch nach Integration ist vorhanden, die technische Voraussetzung dafür oft nicht. Wer bei den Dokumenten anfängt, braucht im ersten Schritt keine Schnittstelle.

Die drei Systeme, an die angeschlossen werden müsste

20/32	19/32	19/32
ERP-System	CRM-System	Microsoft 365 (SharePoint, Teams)

Nur 10 von 32 nennen ein GRC-Modul, nur 8 spezifische Legal-Tech-Werkzeuge. Die relevanten Daten liegen also überwiegend in Systemen, die es ohnehin schon gibt, allen voran in der Microsoft-Umgebung. Das ist eine gute Nachricht: Der erste nutzbringende Schritt braucht keine neue Plattform, sondern Zugriff auf einen definierten Ordner.



Name	Änderungsdatum	Größe	Art
Whitepaper	Heute, 15:53	--	Ordner
Whitepaper_KI_in_Compliance_MMIND_Bratschi_Entwurf_v2.pdf	Heute, 15:37	2.9 MB	PDF-Dokument
KI_in_Compliance_MMIND_2026-08-20.pptx	Gestern, 18:57	1.7 MB	Office...entation
B_Corp_Eligibility_Treuhand_Vaduz.md	Gestern, 08:29	15 KB	Markdown
Beispiel B Corp	Gestern, 03:10	--	Ordner
generator_praesentation.js	Vorgestern, 16:25	29 KB	JavaSc...t script
KI_in_Compliance_MMIND_2026-08-20.pdf	Vorgestern, 16:25	180 KB	PDF-Dokument
certification-navigator.zip	Vorgestern, 16:25	5 KB	ZIP-Archiv
ai-bcorp-team-repo-update.zip	Vorgestern, 16:25	90 KB	ZIP-Archiv
Pruefbericht_und_Korrekturen.md	Vorgestern, 16:25	11 KB	Markdown
Beispiel Konrad	Vorgestern, 14:59	--	Ordner
AI Compliance Webinar 2026 final.pptx	14.08.2026, 13:00	4.5 MB	Office...entation
European Sovereign AI Compliance Hub...EIC Accelerator Partner Discussion.pptx	08.07.2026, 08:50	105 KB	Office...entation
European Sovereign AI Compliance Hub - UK Partner Discussion.pptx	30.06.2026, 02:05	70 KB	Office...entation
comliance survey_teilnehmer-auswertung.md	04.06.2026, 11:51	121 KB	Markdown

Abbildung 8: Ein aufgesetzter Datenordner für einen Compliance-Prozess. Der Einstieg ist eine Ordnerstruktur, kein System.

06 · BETRIEBSRAHMEN

Der Wunsch nach intern kollidiert mit dem Markt.

Die klarste Präferenz der ganzen Umfrage. 50 Prozent wollen KI ausschliesslich intern verarbeiten, weitere 25 Prozent hybrid, zusammen 75 Prozent. Nur 19 Prozent halten eine externe Cloud-Lösung für akzeptabel. Beim Hosting nennen 11 Private Cloud und 7 On-Premises, lediglich 5 nennen SaaS. 13 wollen den Betrieb in der eigenen IT.

Dieser Befund kollidiert mit dem Markt. Nahezu alle leistungsfähigen KI-Werkzeuge sind Cloud-Dienste. Wer «ausschliesslich intern» ernst nimmt, landet bei offenen Modellgewichten im Selbstbetrieb und nimmt dafür einen messbaren Leistungsrückstand in Kauf.

Bei Daten unter einem Berufsgeheimnis kommt ein Punkt hinzu, den viele übersehen: Nach dem Merkblatt der Datenschutzbeauftragten des Kantons Zürich vom Februar 2026 können US-Behörden über den CLOUD Act auf Personendaten zugreifen, auch wenn diese in Rechenzentren in der Schweiz oder im EU/EFTA-Raum liegen. **Eine Datenresidenz in der Schweiz bei einem US-Anbieter löst dieses Problem nicht.**

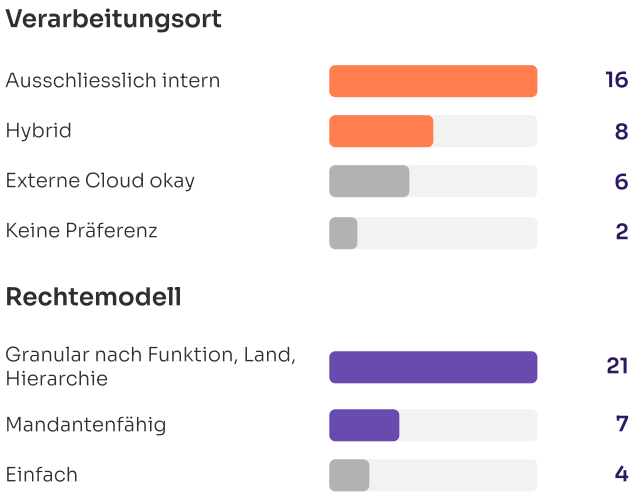


Abbildung 9: 66 Prozent verlangen granulare Rechte. Zusammen mit dem Wunsch nach interner Verarbeitung ergibt das ein Anforderungsprofil, das kein Standard-SaaS-Abo erfüllt.

> Was hier auseinanderläuft, ist auflösbar, aber nur, wenn man die Frage anders stellt. Nicht «welche Plattform kaufen wir?», sondern «welchen einen Prozess bringen wir mit welchen Daten unter welche Kontrolle?»

Ein Wort zu Schatten-KI

Der Befund «ausschliesslich intern» beschreibt einen Wunsch, nicht die Praxis. Wo eine Organisation den Zugang zu geeigneten Werkzeugen nicht regelt, greifen Mitarbeitende zu frei verfügbaren Diensten, mit Unternehmensdaten. Nach dem IBM-Bericht «Cost of a Data Breach 2025» hatten 63 Prozent von 600 befragten Organisationen keine KI-Governance-Richtlinie; 20 Prozent verzeichneten bereits einen Vorfall im Zusammenhang mit Schatten-KI, mit rund 670'000 US-Dollar Mehrkosten pro Fall. Ein Verbot ohne Alternative verlagert das Risiko, es senkt es nicht.

07 · LÖSUNGSEBENEN

Chat, Ordner mit Ablauf, eigene Anwendung.

Wenn heute über KI in Compliance gesprochen wird, ist meist Ebene 1 gemeint: ein Chatfenster. Der Bedarf aus Teil II liegt auf Ebene 2. Ebene 3 bleibt die Ausnahme, und Kapitel 13 sagt, warum.

EBENE 1

Assistenz: das Chatfenster

Eine Frage, eine Antwort. Nützlich für Formulierungen, Übersetzungen, erste Einordnungen. **Löst die Aufgaben aus Teil II nicht:** nichts wird gespeichert, nichts ist wiederholbar, nichts prüfbar. Wer das jährliche Risk Assessment mit einem Chat macht, macht es nächstes Jahr wieder von vorn und kann niemandem zeigen, wie das Ergebnis entstanden ist. Aus Sicht von Aufgabe 3 ist Ebene 1 wertlos: sie produziert keine Belege.

EBENE 2 · HIER LIEGT DER HEBEL

Ordner plus hinterlegter Ablauf

Ein definierter Ordner mit den relevanten Dokumenten, ein schriftlich hinterlegter Arbeitsablauf, ein wiederholbares Ergebnis. Der Ablauf ist eine Textdatei, keine Software. Er beschreibt, welche Quellen zu prüfen sind, in welcher Reihenfolge, nach welchen Kriterien, in welchem Format das Ergebnis entsteht, was zitiert werden muss und wo ein Mensch entscheiden muss.

Das ist die Antwort auf die Umfrage. Wiederholbar, überprüfbar, versionierbar, an einen Ordner gebunden statt an eine Person. Und aufsetzbar in Tagen, nicht in Quartalen. Kapitel 8 und 9 zeigen es konkret.

EBENE 3

Selbstgebaute Anwendung

Eine eigene kleine Applikation mit Oberfläche, für wiederkehrende Aufgaben mit vielen Beteiligten oder grossem Volumen. Heute ohne Entwicklerteam baubar. **Aber:** ab hier entstehen Betreiber- und teilweise Anbieterpflichten, Sicherheitsverantwortung und Wartungslast. Kapitel 10, 11 und 13 zeigen Nutzen und Preis.

Abbildung 10: Die drei Ebenen unterscheiden sich nicht in der Modellqualität, sondern darin, ob das Ergebnis wiederholbar und belegbar ist. Ebene 2 ist der einzige Ort, an dem beides zusammenkommt, ohne dass ein Softwareprodukt entsteht.

Wiederholbar?

Ebene 1 nein
Ebene 2 **ja**
Ebene 3 **ja**

Belegbar für ein Audit?

Ebene 1 nein
Ebene 2 **ja, über Ordner und Version**
Ebene 3 **nur mit gebautem Log**

Aufwand bis zum Nutzen

Ebene 1 Minuten
Ebene 2 Tage
Ebene 3 Wochen bis Monate

08 · EBENE 2

Ihr Werkzeug kann das schon.

Vier Fähigkeitsklassen genügen, um Aufgabe 2 und 3 abzudecken. Alle vier sind 2026 in mehreren Werkzeugen verfügbar, der Ansatz ist also nicht an einen Anbieter gebunden. Wir benennen die Produkte trotzdem, weil man sonst nicht bestellen kann, was man braucht.

FÄHIGKEITSKLASSE	WAS SIE LEISTET	WO SIE HEUTE VERFÜGBAR IST
Hinterlegter Ablauf «Skill»	Eine Textdatei beschreibt einen Arbeitsablauf samt Kriterien, Format, Zitierpflicht und Abbruchbedingungen. Wird bei passender Aufgabe automatisch geladen und abgearbeitet. Versionierbar wie ein Dokument.	Claude Skills · Codex und Gemini über `AGENTS.md` · GitHub Copilot über Custom Instructions · Mistral über Agents und Bibliotheken
Arbeiten im Ordner	Lesen, Vergleichen und Aktualisieren ganzer Dokumentbestände am Ort, an dem sie liegen, statt Datei für Datei hochzuladen. Entscheidend bei den 84 Prozent mit unstrukturierten Dokumenten.	Claude Cowork · Codex CLI · Mistral Vibe CLI · Grok Build CLI · Cursor · Gemini Antigravity
Dauerhafter Kontext «Projekt»	Ein abgegrenzter Raum mit eigenen Dateien, eigenen Regeln und eigener Historie. Die Weisungslage der Organisation liegt darin, nicht im Gedächtnis der Person.	Claude Projects · ChatGPT Projects · Mistral Le Chat Bibliotheken · Copilot Spaces
Zeitgesteuerte Aufgabe	Der Ablauf läuft von selbst: wöchentlich, monatlich, quartalsweise. Aus einer Erinnerung wird ein Prozess. Voraussetzung für Regulatory Monitoring als Regelbetrieb.	Claude Aufgaben und Cowork-Zeitplan · Codex Cloud in CI · jede CLI im Headless-Modus per Cron

Abbildung 11: Fähigkeitsklassen statt Produktnamen. Wer in diesen vier Klassen denkt, bleibt bei Anbieterwechseln handlungsfähig. Stand August 2026; Produktnamen und Funktionsumfang ändern sich schnell.

Wie ein hinterlegter Ablauf tatsächlich aussieht

Auszug, gekürzt

Name: regulatory-monitor
Zweck: Monatlicher Regulatorik-Bericht für die Compliance-Funktion.

Quellen: nur die im Quellenregister gelisteten amtlichen Seiten und Verbandsmitteilungen. Keine anderen.

Ablauf:
1 Quellenregister lesen.
2 Je Quelle Änderungen seit dem letzten Lauf erfassen.
3 Relevanz gegen die Themenliste der Organisation prüfen.
4 Je Treffer: Fundstelle, Datum, wörtliches Zitat, betroffene Weisung.
5 Unklare Fälle als offene Frage ausweisen, nicht bewerten.

Grenzen: keine Rechtsauskunft. Jede Einschätzung ohne Belegstelle wird als solche gekennzeichnet. Vor Versand ist eine menschliche Freigabe erforderlich.

Das ist der ganze Trick, und genau darin liegt die Pointe. Ein Compliance-Ablauf wird nicht programmiert, er wird aufgeschrieben. Wer eine Weisung formulieren kann, kann einen solchen Ablauf formulieren.

Drei Eigenschaften machen ihn auditfähig, und alle drei sind bewusst gesetzt. Erstens die **Quellenbindung**: die Menge der zulässigen Quellen ist geschlossen. Zweitens die **Belegpflicht**: jede Aussage trägt eine Fundstelle, sonst wird sie als Einschätzung markiert. Drittens der **Haltepunkt**: an definierter Stelle entscheidet ein Mensch.

Ohne diese drei Eigenschaften entsteht kein Compliance-Werkzeug, sondern ein Textgenerator mit Compliance-Vokabular. Der Unterschied wird in Kapitel 13 mit Zahlen unterlegt.

So sieht das in der Praxis aus

Drei Ansichten aus dem Zertifizierungs-Navigator, den Kapitel 9 beschreibt: der Aufruf, die Definition des Ablaufs, und das Repository, über das ein freigegebener Ablauf im Team verteilt wird.

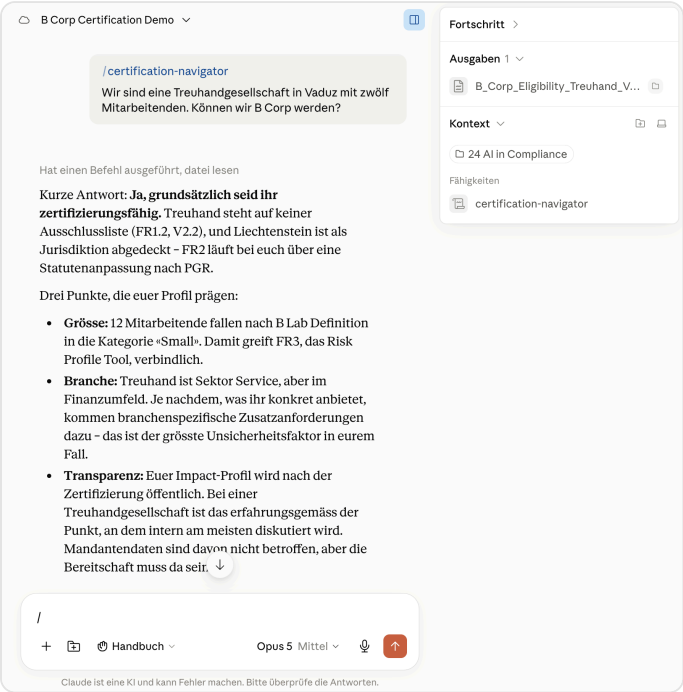


Abbildung 12: Der Aufruf. Die Fachperson beschreibt ihr Anliegen in normaler Sprache. Der passende Ablauf wird automatisch geladen. Ein Kommando muss niemand lernen.

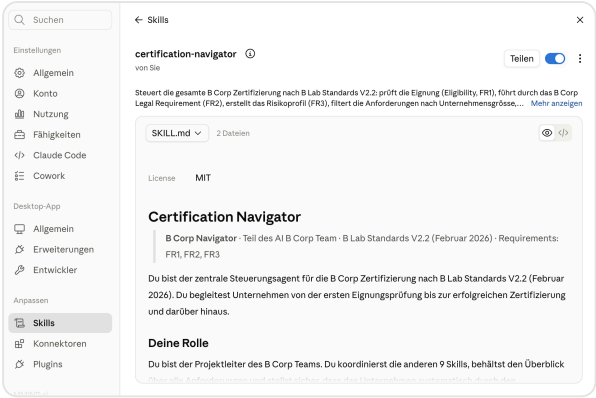


Abbildung 13: Der Ablauf selbst: eine Textdatei mit Zweck, Auslösebegriffen, Schritten, Referenzmaterial und Grenzen. Lesbar und änderbar für jede Person, die eine Weisung formulieren kann.

Warum das Repository der Hebel ist

Ein Ablauf ist eine Textdatei. Damit gilt für ihn, was für jedes Dokument unter Versionskontrolle gilt: Änderungen sind nachvollziehbar, frühere Fassungen bleiben abrufbar, Freigaben laufen über einen dokumentierten Prüfschritt.

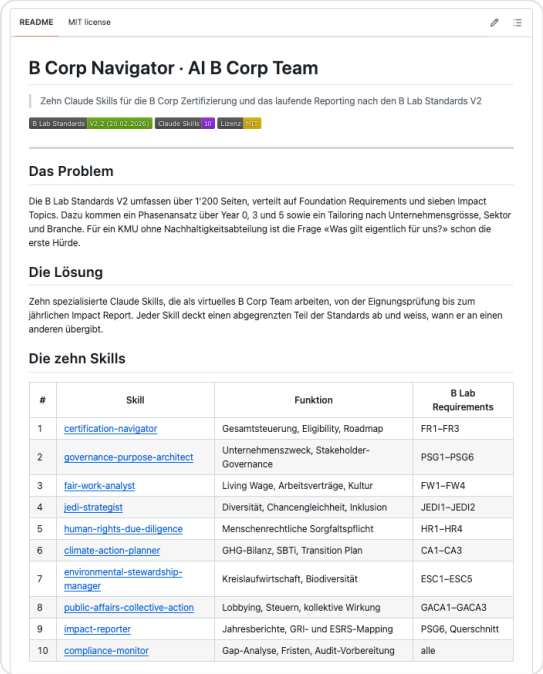


Abbildung 14: Dieselben Abläufe in einem Git-Repository.

Praktisch heisst das: Ein Ablauf, den die Konzern-Compliance einmal geprüft und freigegeben hat, lässt sich über ein Repository an alle Tochtergesellschaften verteilen. Wird die Weisung geändert, ändert sich der Ablauf an einer Stelle. Das adressiert die 66 Prozent, die granulare Rechte verlangen, und die 22 Prozent mit Mandantenanforderungen.

Für ein Audit ist das der entscheidende Punkt. Nicht «wir haben KI benutzt», sondern: hier ist die freigegebene Fassung, hier die Änderungshistorie, hier der Lauf, der diesen Bericht erzeugt hat.

Der Unterschied zu Ebene 1: Am Ende liegt kein Text vor, sondern ein Nachweis. Dieselbe Frage, morgen gestellt, führt über denselben Weg und lässt sich gegen die freigegebene Fassung prüfen.

09 · FALLBEISPIEL A · EBENE 2

Ein Normwerk statt drei Tage Lesearbeit.

12
Mitarbeitende, Anstalt nach PGR, Vaduz

7.9 MB
Normwerk als PDF-Grundlage (B Lab Standards)

1 Ordner
plus ein hinterlegter Ablauf, keine Software

0 Zeilen
Programmcode im Einsatz

Die Aufgabe

Eine Treuhandgesellschaft in Vaduz mit klassischer Treuhand, Buchhaltung, Steuern und Vermögensverwaltung wollte wissen, ob und unter welchen Bedingungen eine B-Corp-Zertifizierung möglich ist. Die Grundlage sind die B Lab Standards in Version 2.2 vom 20. Februar 2026: ein mehrhundertseitiges, versioniertes Normwerk mit Foundation Requirements, branchen- und grössenabhängigem Zuschnitt und Fristen in Jahr 0, 3 und 5.

Von Hand ist das mehrtägige Lesearbeit, mit dem realen Risiko, eine branchenspezifische Zusatzanforderung zu übersehen. Genau das ist der Vorgang, den 22 von 32 Befragten beschreiben: Text lesen, Relevanz beurteilen, zusammenfassen.

Der Aufbau

Ein Ordner mit dem Normwerk und einer für die Weiterverarbeitung aufbereiteten Textfassung. Daneben ein hinterlegter Ablauf mit Anforderungsmatrix als Referenzdatei, bewusst so gebaut, dass die Matrix erst gelesen wird, wenn eine konkrete Requirement-ID gebraucht wird.

Das Ergebnis

Eignungsbericht, Stand 20.08.2026. Vier von fünf Bedingungen des Foundation Requirements FR1 als erfüllt belegt, eine als Entscheidung der Geschäftsleitung ausgewiesen.

Der eigentliche Fund. B Lab kennt keine Branche «Treuhand». Die Vermögensverwaltung fällt aber unter **Investment advising**. Damit greifen zwei branchenspezifische Zusatzanforderungen ab Jahr 0: eine dokumentierte Menschenrechtsprüfung und eine Umweltprüfung der Investments, je für die drei materiellsten Positionen pro Jahr. Beide gelten unabhängig von der Unternehmensgrösse. Eine Anstalt mit 12 Mitarbeitenden trifft dasselbe wie einen grossen Asset Manager.

Und eine ehrliche Lücke. Der Bericht weist selbst aus, dass die Zurechnungslogik in Version 2.2 gegenüber 2.1 geändert wurde und dieser Punkt noch zu verifizieren ist. Das ist kein Mangel, das ist die Funktion: der Ablauf ist angewiesen, Unsicherheit zu markieren statt zu überschreiben.

Was daran übertragbar ist

Der Fall ist kein B-Corp-Fall. Er ist der Prototyp für jede Aufgabe der Form **«öffentliches, versioniertes Normwerk trifft konkretes Unternehmensprofil»**, und damit für einen grossen Teil der 72 Prozent zum jährlichen Risk Assessment. ISO 37301, ein FINMA-Rundschreiben, ein Verhaltenskodex einer Konzernmutter, eine Lieferantenanforderung: dasselbe Muster, dasselbe Vorgehen. Der Grund, warum es funktioniert, ist die Struktur der Quelle: öffentlich, versioniert, tabellarisch. Damit bleibt jeder Fehler nachprüfbar.

Vom Ordner zum Nachweis

SCHRITT 1

Ordner

Normwerk, aufbereitete Textfassung, Unternehmensangaben. Alles an einem Ort, versioniert.

SCHRITT 2

Ablauf

Eignung prüfen, Rechtsanforderung, Risikoprofil, Anforderungen nach Profil filtern, Roadmap bauen.

SCHRITT 3

Bericht

Eignung, gefilterte Anforderungsmatrix, Roadmap Jahr 0, 3 und 5, mit Belegstellen und markierten Unsicherheiten.

SCHRITT 4

Freigabe

Statutenanpassung und Rechtsfragen gehen an die Juristin. Der Ablauf sagt das selbst.

Abbildung 15: Der Haltepunkt in Schritt 4 ist Teil der Konstruktion, nicht ein Zugeständnis. Ein Ablauf, der seine eigenen Grenzen kennt, ist der einzige, den man in einem regulierten Umfeld einsetzen kann.

B Corp Eligibility Report

Unternehmen: Treuhandgesellschaft, Vaduz (Liechtenstein) **Rechtsform:** Anstalt (PGR) **Mitarbeitende:** 12 **Leistungen:** Klassische Treuhand · Buchhaltung und Steuern · Vermögensverwaltung **Operativ seit:** über 5 Jahre **Stand:** 20.08.2026 · B Lab Standards V2.2 (20.02.2026)

---

1. Ergebnis: Eignung bestätigt

Ihr könnt B Corp werden. Es gibt kein strukturelles Hindernis. Alle vier Bedingungen des Foundation Requirements FR1 sind erfüllt oder erfüllbar:

Kriterium	Status	Bemerkung
Mindestens 12 Monate operativ (FR1.1)	erfüllt	über 5 Jahre
Umsatz aus kompetitivem Markt (FR1.1)	erfüllt	Treuhanddienstleistungen am Markt
Kein Branchenausschluss (FR1.2)	erfüllt	siehe Abschnitt 2
Gesetzeskonformität (FR1.3, FR1.4)	vorausgesetzt	intern zu bestätigen
Transparenzbereitschaft (FR1.5)	zu entscheiden	siehe Abschnitt 5

Abbildung 16: Der erzeugte Eignungsbericht. Ergebnistabelle zu FR1, die Einordnung der Vermögensverwaltung als Investment advising und der selbst ausgewiesene Versionsvorbehalt zu V2.2. Wer prüfen will, findet zu jeder Aussage die Fundstelle.

10 · EBENE 3

Wann sich eine eigene Anwendung lohnt.

Ebene 2 endet dort, wo viele Personen dasselbe wiederholt tun, wo ein Zustand über Monate fortgeschrieben wird oder wo Dritte etwas eingeben sollen. Dann braucht es eine Oberfläche, und die ist 2026 ohne Entwicklerteam baubar. Der Preis dafür ist Verantwortung. Der wird selten mitgerechnet.

Wofür sich Eigenbau in Compliance anbietet

ANWENDUNGSKLASSE	WARUM SIE SICH ANBIETET	EINSCHÄTZUNG
Policy-Diff: Weisungen gegen neue Fassung vergleichen	Der Vergleich ist deterministisch, das Ergebnis in Sekunden vom Menschen prüfbar. Adressiert die 44 Prozent, die Policy Management nennen, und den Freitextbefund «Aktualisierung Manuals/Reglemente».	**Eigenbau vertretbar**
Schulungsnachweis-Tracker	50 Prozent nennen die Überwachung von Schulungsnachweisen. Zugleich ist die KI-Kompetenzpflicht nach Artikel 4 EU-AI-Act seit dem 2. Februar 2025 selbst eine Nachweispflicht. Der Anwendungsfall trägt sich also doppelt.	**Eigenbau vertretbar**
Zertifizierungs-Navigator	Öffentlicher, versionierter, tabellarischer Anforderungskatalog. Fehler bleiben nachprüfbar. Siehe Fallbeispiel A, dort auf Ebene 2 gelöst.	**Vertretbar mit Endkontrolle**
ESG- und Nachhaltigkeits-One-Pager	Grosse Dokumentmengen, feste Normwerte, rechenbares Ergebnis. Siehe Fallbeispiel B.	**Vertretbar mit Endkontrolle**
Geschäftspartnerprüfung / Third Party Due Diligence	50 Prozent nennen es. Aber: Personendaten, Bewertungen mit Rechtsfolge, Nähe zu Anhang III des EU-AI-Act. Datenschutz-Folgenabschätzung zwingend prüfen.	**Nur mit DSFA und Rechtsprüfung**
Regulatory Watchlist	Höchster Bedarf (81 Prozent recherchieren manuell), zugleich höchstes Halluzinationsrisiko genau in der Domäne, in der es am teuersten ist.	**Nur als Signalgeber, nie als Auskunft**

Abbildung 17: Priorisierung nach dem Verhältnis von Nutzen zu Risiko, nicht nach Attraktivität. Für keine dieser Klassen existiert eine öffentlich dokumentierte, namentliche Fallstudie eines selbstgebauten Werkzeugs. Belegt sind der Bedarf und der Aufgabenumfang; die Reihenfolge ist unsere Einschätzung.

HOHER NUTZEN · GERINGES RISIKO

- Policy-Diff
- Schulungsnachweis-Tracker
- Berichtsvorlage aus Rohdaten

Hier anfangen.

HOHER NUTZEN · HOHES RISIKO

- Regulatory Watchlist
- Third Party Due Diligence
- Hinweisgeber-Auswertung

Nur mit Governance und Rechtsprüfung.

GERINGER NUTZEN · GERINGES RISIKO

- Textbausteine, Übersetzungen
- Protokoll-Zusammenfassungen

Nützlich, aber kein Projekt.

GERINGER NUTZEN · HOHES RISIKO

- Automatische Rechtsauskunft
- Vollautomatische Freigabeentscheide
- Anomalie-Alarme ohne Prüfpfad

Nicht angehen.

Abbildung 18: Nutzen-Risiko-Matrix für Compliance-Anwendungen, in der Logik der Aufwand-Nutzen-Matrix aus dem MMIND-Leitfaden Digitalisierung. Bemerkenswert: der häufigste Wunsch der Umfrage (KI-erkannte Anomalien, 81 Prozent) landet ohne Prüfpfad im Feld unten rechts.

11 · FALLBEISPIEL B · EBENE 3

Nachhaltigkeitsbericht in 45 Minuten statt drei Tagen.

Umgesetzt mit der Hanno Konrad Anstalt, Ingenieure, Planer und Geometer. Ein Prototyp, der aus unstrukturierten Projektdokumenten einen belegten Nachhaltigkeitsbericht erzeugt.

45 Min.

Verarbeitung für ein Projekt mit 1'200 bis 1'500 Seiten Projektdokumenten

0.20 bis 0.50 CHF

Modellkosten pro Durchlauf

>800 Seiten

Normendokumente von KBOB, ecobau, SIA und SNBS als Referenz

Die Aufgabe

KMU der Baubranche stehen unter doppeltem Druck. Die Anforderungen an Nachhaltigkeitsberichterstattung steigen, und grosse berichtspflichtige Auftraggeber geben diesen Druck weiter. Ein Bericht für ein einzelnes Bauprojekt band mehrere Tage Arbeitszeit einer qualifizierten Projektleitung.

Was gebaut wurde

Eine Webanwendung, die Devis, Rechnungen und Baubeschriebe einliest, Materialien und Mengen extrahiert, ihnen CO_2-Äquivalente aus KBOB-, ecobau-, SIA- und SNBS-Normdokumenten zuordnet, rechnet und gegen die Nachhaltigkeitskriterien prüft.

Dieselbe Aufgabenstruktur (unstrukturierte Dokumente, festes Normwerk, rechenbares Ergebnis, Belegpflicht) liegt bei 84 Prozent der Befragten vor.

Die Entscheidungen, auf die es ankam

1. **Vollständige Quellenangaben**

   Jede Aussage trägt Dokumentname und wörtliches Zitat. Ohne diese Entscheidung wäre der Bericht nicht prüfbar und für Compliance wertlos.

2. **Klärungsfragen statt Annahmen**

   Wo Angaben fehlen oder widersprüchlich sind, fragt das Werkzeug nach, statt zu schätzen. Im Prototyp etwa bei einer Bewehrungsmenge, die im Devis unplausibel angegeben war.

3. **Versionierung mit Prüfpfad**

   Jede Version wird mit Zeitstempel gespeichert, frühere Fassungen bleiben abrufbar. Antwort auf Artikel 26 EU-AI-Act.

4. **Menschliche Prüfung als Pflichtschritt**

   Der erste Bericht ist ausdrücklich ein Entwurf. Erfahrungsgemäss erreicht erst die zweite oder dritte Fassung die Qualität für eine offizielle Verwendung.

Abbildung 19: Gesamtbewertung eines realen Projekts, hier 74 Punkte und Silber-Standard. Darunter folgt je Dimension eine Begründung mit Werten und Normbezug, etwa «3-fach Verglasung Uw 0.87 W/m²K nach SIA 380/1». Wo Nachweise fehlen, weist das Werkzeug es aus, im Beispiel bei den RC-Beton-Nachweisen im Ortbetonbau.

Was wir dabei gelernt haben, auch das Unbequeme

Funktioniert hat

- Zweistufige Analyse: schnelles Modell für Zusammenfassungen, starkes Modell für die Endauswertung. Senkt Kosten und Laufzeit deutlich.
- Strukturierte Ausgabe nach festem Schema statt Freitext. Ohne das ist Datenextraktion nicht zuverlässig.
- Transparenz schafft Vertrauen schneller als Genauigkeit. Ein sichtbar markierter Zweifel überzeugt mehr als eine glatte Zahl.
- Ordnerdisziplin auf Nutzerseite: Projektdaten und Normdokumente getrennt. Derselbe Punkt wie in Fallbeispiel A.

Nicht funktioniert hat oder teuer war

- Die erste Fassung war nie die brauchbare. Iteration ist kein Nachbessern, sondern Teil des Verfahrens.
- Browserbasierte Speicherung senkt die Einstiegshürde, ist aber keine Grundlage für Mehrbenutzerbetrieb und Aufbewahrungspflichten.
- Die Genauigkeitsziele (mindestens 90 Prozent bei CO_2-Berechnungen, unter 5 Prozent kritische Fehler) sind gesetzte Zielwerte aus der Testphase, keine unabhängig geprüften Ergebnisse. Wir weisen sie deshalb als Ziele aus.
- Ab dem Moment, in dem Dritte die Anwendung nutzen, entstehen Pflichten, die vorher niemand auf der Rechnung hatte. Siehe Kapitel 13.

Die ehrliche Einordnung der 80 Prozent

Der Prototyp wirbt mit bis zu 80 Prozent Zeitersparnis. Diese Zahl stammt aus unserer eigenen Messung an realen Projekten und ist nicht extern validiert. Sie gilt zudem für den Erstellungsschritt, nicht für den ganzen Prozess. Die menschliche Prüfung bleibt und ist in der Rechnung nicht vollständig abgebildet. Wir nennen die Zahl trotzdem, weil sie die Grössenordnung richtig trifft. Aber sie ist eine Erfahrung, kein Beweis. Wer in seiner eigenen Organisation entscheidet, sollte einen eigenen Vergleich an zwei oder drei realen Fällen rechnen, bevor er investiert.

Was das für eine Compliance-Funktion bedeutet

Der Prototyp ist der Business Case

Am Anfang stand keine Investitionsrechnung, sondern ein Prototyp an echten Projektdaten. Erst der zeigte, ob die Extraktion trägt. Diese Reihenfolge ist billiger als jede Vorstudie.

Die Begründungspflicht ist die Qualitätskontrolle

Ein Modell, das jede Zahl mit Fundstelle und Normbezug belegen muss, kann weniger frei erfinden. Was übrig bleibt, fällt beim Lesen auf. Ohne diese Auflage fällt es nicht auf.

Ebene 3 braucht einen Eigentümer

Sobald Dritte die Anwendung nutzen, braucht sie eine benannte verantwortliche Person, ein Sicherheitsreview und eine Aufbewahrungsregel. Wer das nicht besetzen kann, bleibt besser auf Ebene 2.

Der eigentliche Ertrag von Fallbeispiel B war nicht der Bericht. Es war die Erkenntnis, dass die Aufgabenstruktur in Compliance immer dieselbe ist: Dokumente, Normwerk, Belegpflicht, menschliche Freigabe. Wer sie einmal gebaut hat, baut sie wieder.

12 · ANBIETER

Entscheidend ist, wo Ihre Dokumente liegen.

Der Markt hat sich 2026 auf zwei Achsen sortiert. Die erste (wie gut ein Modell Code und Text produziert) ist für Compliance-Aufgaben selten der Engpass. Die zweite entscheidet: wo Ihre Dokumente physisch und rechtlich liegen.

WERKZEUG	KLASSE	DATENRESIDENZ EU / CH	FÜR CH UND FL RELEVANT
Claude Skills, Cowork, Projects, Aufgaben	Ordnerarbeit, hinterlegter Ablauf, Zeitplan	Cloud; Enterprise-Optionen prüfen	Reifste Umsetzung des hinterlegten Ablaufs und der Ordnerarbeit. Kein Selbstbetrieb.
OpenAI Codex	CLI, Cloud-Agent	**«Europe (EEA + Switzerland)»**, Region nur bei Projekterstellung wählbar, später nicht änderbar	Einer von zwei Anbietern im Feld, die die Schweiz namentlich einschliessen. CLI unter Apache 2.0. Kein On-Premises.
GitHub Copilot	Agent in der Entwicklungsumgebung	**EU Data Boundary inkl. EFTA**, Schweiz und Liechtenstein seit 1. Mai 2026, Aufschlag 10 Prozent	Formal die beste Abdeckung. Ob der eigentliche Coding-Agent darunter läuft, ist widersprüchlich dokumentiert. Vor Einsatz schriftlich bestätigen lassen.
Mistral	Chat, CLI, offene Gewichte	**EU-Sitz, On-Premises-Option**	Der einzige Anbieter mit EU-Sitz, On-Premises, offener CLI und offenen Gewichten. Deckt «ausschliesslich intern» real ab. Preis für On-Premises nicht öffentlich, Leistung unter dem Spitzenfeld.
Kimi / Moonshot	API, offene Gewichte	Sitz Peking, keine Zusagen	Interessant nur über die offenen Gewichte im Selbstbetrieb. API-Nutzung bedeutet Datenexport nach China ohne Angemessenheitsbeschluss.
Offene Modelle im Selbstbetrieb	eigene Infrastruktur	**volle Kontrolle**	Die einzige Variante, die den CLOUD Act ausschliesst. Leistungsrückstand real, Betriebsaufwand vollständig intern.

Abbildung 20: Auswahl, Stand 21. August 2026, aus öffentlichen Quellen und Herstellerangaben. Preise und Funktionsumfang ändern sich monatlich; die Tabelle ist als Prüfraster gedacht, nicht als Einkaufsliste. Vollständige Quellenangaben in Anhang B.

Eine brauchbare Entscheidungsregel

Statt Anbieter zu vergleichen, klassifizieren Sie zuerst die Daten. Danach ist die Auswahl in den meisten Fällen eindeutig.

DATENKLASSE A

Öffentlich

Gesetzestexte, Normwerke, Verbandsmitteilungen, veröffentlichte Berichte.

Regel: jedes leistungsfähige Cloud-Werkzeug ist zulässig. Hier fängt man an, und hier liegt der grösste Teil von Aufgabe 1.

DATENKLASSE B

Intern, ohne Personenbezug

Eigene Weisungen, Prozessbeschreibungen, anonymisierte Kennzahlen.

Regel: Cloud mit EU- oder CH-Datenresidenz, vertraglich zugesichert, kein Training auf den Daten, Aufbewahrungsfristen geklärt.

DATENKLASSE C

Personenbezogen oder geheimnisgeschützt

Hinweisgebermeldungen, Untersuchungsakten, Kundendaten, Berufsgeheimnis.

Regel: Selbstbetrieb offener Gewichte oder ein Hoster ohne US-Konzernmutter. Datenresidenz allein genügt hier nicht, siehe unten.

Abbildung 21: Datenklassen als Auswahlfilter. Die praktische Konsequenz ist angenehm: Aufgabe 1 und ein grosser Teil von Aufgabe 2 lassen sich in Klasse A und B umsetzen, also sofort und ohne Infrastrukturprojekt.

Der Befund, der die meisten überrascht

Nach dem Merkblatt der Datenschutzbeauftragten des Kantons Zürich vom Februar 2026 können US-Behörden über den CLOUD Act auf Personendaten zugreifen, auch wenn diese in Rechenzentren in der Schweiz oder im EU/EFTA-Raum liegen, ohne Zustimmung des Belegenheitsstaats und unter Umgehung der Rechtshilfe. Bei Berufs-, Steuer-, Sozialhilfe- und Opferhilfegeheimnissen sind zudem auch Randdaten zu schützen. Für Datenklasse C heisst das: die Frage «liegen die Daten in der Schweiz?» ist die falsche Frage. Die richtige lautet «wessen Recht greift auf den Betreiber zu?».

Wer die Datenklasse zuerst klärt, spart sich die Anbieterdiskussion. Wer mit der Anbieterdiskussion anfängt, führt sie zweimal.

13 · GRENZEN

Risiken, die den Einsatz begrenzen.

Ein Compliance-Papier ohne Gegenposition wäre wertlos. Nichts in diesem Kapitel widerlegt Teil III. Alles darin bestimmt, wie man vorgeht.

Halluzination in Rechtsfragen ist nicht gelöst

Die erste präregistrierte Untersuchung spezialisierter Rechts-KI-Werkzeuge (Stanford RegLab) fand Halluzinationsraten von 17 bis 33 Prozent, und zwar bei Werkzeugen mit Zugriff auf kuratierte Rechtsdatenbanken. Ein selbstgebautes Werkzeug auf einem Allzweckmodell wird kaum besser abschneiden.

Zur Kalibrierung: Stand 9. Juni 2026 sind weltweit 1'598 Gerichtsfälle mit KI-erfundenen Zitaten dokumentiert, mit steigender Tendenz. Sanktionen reichen von wenigen Tausend bis über 100'000 US-Dollar, in Einzelfällen bis zu Suspendierungen.

Konsequenz: Regulatory Monitoring ausschliesslich als Signalgeber mit Pflicht zur Quellenverifikation. Niemals als Rechtsauskunft, niemals ohne Fundstelle.

Selbstgebaute Anwendungen sind oft faktisch offen

Ein Scan von 5'600 mit KI gebauten Produktivanwendungen fand keine einzige mit CSRF-Schutz und keine mit üblichen Sicherheits-Headern. Eine zweite Untersuchung fand rund 5'000 Anwendungen mit fehlkonfigurierten Zugriffseinstellungen, davon etwa 40 Prozent praktisch ohne Authentifizierung. Exponiert waren unter anderem Spitalpläne und Verkaufsdaten.

Ergänzend: KI-erzeugter Code enthielt in 44 Prozent der Generierungsaufgaben eine sicherheitsrelevante Schwachstelle; die Sicherheits-Erfolgsquote lag bei 56 Prozent und ist gegenüber dem Vorjahr praktisch unverändert.

Konsequenz: Ebene 3 nie ohne Sicherheitsprüfung durch Dritte in Betrieb nehmen. Prototypen von Beginn an als öffentlich zugänglich annehmen.

Wer selbst baut, wird zum Anbieter

Der übersehene Mechanismus: Nach Artikel 25 EU-AI-Act wird zum Anbieter eines Hochrisikosystems, wer seinen Namen darauf setzt, eine wesentliche Änderung vornimmt oder die Zweckbestimmung so ändert, dass ein System hochriskant wird. Artikel 26 verlangt von Betreibern menschliche Aufsicht durch fachlich befähigte Personen, die Aufbewahrung automatisch erzeugter Protokolle für mindestens sechs Monate und die Information der Arbeitnehmenden vor dem Einsatz am Arbeitsplatz. Artikel 4 verlangt seit dem 2. Februar 2025 Massnahmen zur KI-Kompetenz, auch bei rein interner Nutzung.

Der Zeitplan ist in Bewegung

Der AI-Act-Omnibus, Verordnung (EU) 2026/1744, ist seit dem 27. Juli 2026 in Kraft. Er verschiebt die Hochrisiko-Pflichten: Anhang III auf den 2. Dezember 2027, Anhang I auf den 2. August 2028. Die Transparenzpflichten nach Artikel 50 gelten ab dem 2. August 2026. **Wichtig:** Generative Systeme, die schon vorher auf dem Markt waren, müssen Absatz 2 erst ab dem 2. Dezember 2026 erfüllen. Ältere Analysen nennen weiterhin den 2. August 2026 für Hochrisiko. Für Liechtenstein gilt zudem: die Verordnung ist noch nicht ins EWR-Abkommen übernommen.

14 · VOM BEDARF ZUR UMSETZUNG

Erst optimieren, dann digitalisieren.

Das Vorgehen ist keine Erfindung für dieses Papier. Es ist die Digitalisierungsmethodik aus dem MMIND-Leitfaden, den wir mit dem Schweizerischen Institut für KMU und Unternehmertum der Universität St. Gallen erarbeitet haben, angewendet auf einen Compliance-Kernprozess. Der Grundsatz von dort gilt hier unverändert: **erst optimieren, dann digitalisieren.**

1

Use Cases und Quick Wins definieren

Alle Kandidaten aus dem Alltag sammeln und in der Aufwand-Nutzen-Matrix verorten: Quick Wins sofort, grosse Projekte geplant, Zeitfresser gar nicht. Für die Compliance-Funktion kommt eine dritte Achse hinzu, die im Leitfaden nicht nötig war: die Datenklasse aus Kapitel 12. Ein Quick Win in Datenklasse C ist kein Quick Win.

Ergebnis: priorisierte Liste mit drei bis fünf Kandidaten, einer davon als erster Prozess entschieden. Dauer: ein halber Tag.

2

Prozessanalyse für den Kernprozess

Ist-Zustand aufnehmen: wer macht was, womit, mit welchen Daten, an welcher Stelle bricht das Medium. Dann Soll-Zustand nach den drei Fragen aus dem Leitfaden: **Eliminieren:** welcher Schritt ist verzichtbar? **Vereinfachen:** welche Schritte lassen sich zusammenfassen? **Standardisieren:** wie sieht der einheitliche Ablauf aus? Erst dieser dritte Punkt macht den Prozess überhaupt automatisierbar. Ein Prozess, der nicht standardisiert ist, lässt sich nicht hinterlegen.

Ergebnis: Ist/Soll auf einer Seite, Entscheidungspunkte und Haltepunkte markiert. Dauer: ein Tag.

3

Ordner mit den relevanten Daten aufsetzen

Der unterschätzte Schritt, und in beiden Fallbeispielen der, der über die Qualität entschied. Konkret: Quellenregister mit der abschliessenden Liste zulässiger Quellen. Getrennte Unterordner für eigene Dokumente und externe Normwerke. Zugriffsrechte gemäss dem granularen Modell, das 66 Prozent verlangen. Datenklasse pro Ordner festgelegt und dokumentiert.

Ergebnis: lauffähige Ordnerstruktur mit Quellenregister und dokumentierter Datenklasse. Dauer: ein halber Tag, plus Zuliefern durch die Organisation.

4

Ablauf aufsetzen, der den Prozess abarbeitet

Der Soll-Prozess aus Schritt 2 wird zur hinterlegten Anweisung, mit den drei nicht verhandelbaren Eigenschaften aus Kapitel 8: geschlossene Quellenmenge, Belegpflicht, Haltepunkt für die menschliche Entscheidung. Dann zweimal an realen Fällen durchlaufen, nachschärfen, und als zeitgesteuerte Aufgabe einrichten.

Ergebnis: ein laufender, wiederholbarer Prozess mit prüfbarem Ergebnis, plus die Zeitmessung gegen den alten Ablauf. Dauer: ein Tag, plus zwei Testläufe.

Was am Ende vorliegt

Vier Schritte, vier überprüfbare Artefakte. Kein Konzeptpapier, sondern ein laufender Prozess und die Fähigkeit, den nächsten selbst zu bauen.

ARTEFAKT 1

Priorisierte Use-Case-Liste

Mit Aufwand, Nutzen und Datenklasse je Kandidat. Die Grundlage für alle weiteren Entscheide.

ARTEFAKT 2

Ist/Soll des Kernprozesses

Auf einer Seite, mit eliminierten und zusammengefassten Schritten. Nützlich auch ohne KI.

ARTEFAKT 3

Aufgesetzter Datenordner

Quellenregister, Struktur, Rechte, Datenklasse. Wiederverwendbar für jeden weiteren Prozess.

ARTEFAKT 4

Laufender Ablauf

Getestet, zeitgesteuert, mit Belegpflicht und Haltepunkt. Plus gemessene Zeitersparnis.

Abbildung 22: Die vier Artefakte des Workshops. Artefakt 2 und 3 behalten ihren Wert unabhängig davon, welches Werkzeug später eingesetzt wird. Das ist beabsichtigt.

Für wen das funktioniert

Die Methodik setzt keine IT-Kenntnisse voraus. Wer eine Weisung formulieren und einen Prozess beschreiben kann, kann Schritt 4 mitgestalten. Darin liegt der Bruch mit früheren Digitalisierungsprojekten.

Sinnvoll ist die Besetzung mit der Compliance-Verantwortung, einer Person aus dem betroffenen Fachbereich und jemandem mit Zugriff auf die Datenablage. Die IT wird informiert und nicht beauftragt, solange man in Datenklasse A und B bleibt.

Was wir nicht versprechen

Keine vollständige Automatisierung. Keine Ersetzung von Rechtsberatung. Kein Werkzeug, das ohne Prüfung produktiv geht. Und keine Zahl, die wir nicht selbst gemessen haben.

Was wir versprechen: nach vier Schritten läuft ein Prozess, der vorher von Hand lief, und die Organisation kann den nächsten selbst aufsetzen. Das ist der Unterschied zwischen einem Werkzeug und einer Fähigkeit.

> Beginnen Sie nicht mit dem komplexesten Prozess, sondern mit einem Quick Win. Frühe sichtbare Erfolge sind wichtiger als perfekte erste Ergebnisse. auch das eine Erkenntnis, die aus dem Leitfaden Digitalisierung stammt und sich hier bestätigt hat.

15 · GOVERNANCE

Governance-Minimum vor dem ersten Ablauf.

53 Prozent nennen fehlende interne KI-Governance-Expertise als grösste Hürde. Diese Liste ist kein Governance-Rahmenwerk. Sie ist das Minimum, ohne das wir keinen Workshop beginnen.

1. **Freigegebene Werkzeuge benennen**
   Eine kurze Liste zulässiger Werkzeuge je Datenklasse. Verbot ohne Alternative erzeugt Schatten-KI, es verhindert sie nicht.

2. **Datenklassen definieren**
   A öffentlich, B intern ohne Personenbezug, C personenbezogen oder geheimnisgeschützt. Drei Klassen genügen für den Anfang.

3. **Protokollierung sicherstellen**
   Wer hat was wann mit welchem Werkzeug erzeugt. Artikel 26 EU-AI-Act nennt mindestens sechs Monate; Finanzinstitute prüfen die sektorspezifischen Fristen.

4. **KI-Kompetenz nachweisen**
   Artikel 4 gilt seit dem 2. Februar 2025 für Anbieter und Betreiber, auch bei rein interner Nutzung. Eine kurze Schulung mit Teilnahmenachweis erfüllt den Kern.

5. **Haltepunkte festlegen**
   Welche Entscheidung darf nie ohne Menschen fallen. Für Compliance mindestens: Rechtsauslegung, Sanktionsentscheide, externe Kommunikation, Meldungen an Behörden.

6. **Rollen und Rechte spiegeln**
   Der Ordner darf nicht mehr sichtbar machen als die Person ohnehin sehen darf. 66 Prozent verlangen granulare Rechte. Das gilt auch für den Datenordner eines Ablaufs.

7. **Arbeitnehmende informieren**
   Artikel 26 verlangt die Information der Arbeitnehmenden und ihrer Vertretung vor dem Einsatz am Arbeitsplatz. Früh und aktiv gemacht, wird daraus ein Vertrauensgewinn statt einer Pflichtübung.

Aufwand für alle sieben Punkte: nach unserer Erfahrung ein bis zwei Tage für eine mittelgrosse Organisation, vorausgesetzt, jemand entscheidet. Genau dort scheitert es meist, nicht an der Komplexität.

Abbildung 23: Governance-Minimum. Die Punkte 3, 4, 5 und 7 sind regulatorisch verankert, die Punkte 1, 2 und 6 sind praktische Voraussetzung.

ANHANG A

Topline je Frage.

Alle Werte n=32, sofern nicht anders angegeben. Mehrfachauswahl als Anzahl Nennungen, die Summe übersteigt deshalb regelmässig 32. Bedingte Fragen mit reduzierter Basis sind ausgewiesen.

FRAGE	VERTEILUNG
Branche	Finanzdienstleistungen 9 · Industrie/Produktion 9 · Gesundheitswesen 4 · Bau/Immobilien 3 · Öffentliche Verwaltung 3 · Handel 2 · Energie 1 · Sonstiges 1
Organisationsgrösse	über 1'000 Mitarbeitende 16 · 300–1'000 7 · 1–49 5 · 250–299 2 · 50–249 2
Compliance-Kultur	in Standardprozesse integriert 14 · eher reaktiv 6 · proaktiv gelebt 5 · reine Pflichterfüllung 4 · gelebter Wettbewerbsvorteil 3
Zeitaufwand pro Woche	5–19 h 12 · 20–49 h 12 · unter 5 h 4 · 50–100 h 3 · über 100 h 1
Top-Compliance-Themen	Datenschutz 20 · Korruption und Bestechung 17 · interne Richtlinien 17 · Interessenkonflikte 14 · interne Kontrollen 12 · Lieferketten-Sorgfaltspflichten 11 · Geldwäscherei 10 · Fraud 9 · Kartellrecht 8 · Exportkontrolle und Sanktionen 8 · Arbeitssicherheit 7 · ESG 7 · KI-Regulatorik 5
Stand der KI-Regulierung	erste Abklärungen 12 · Governance etabliert 9 · beobachten ohne Massnahmen 9 · noch kein Thema 2
Hürden bei KI-Compliance	fehlende interne Expertise 17 · Klassifizierung eigener Systeme 15 · unklare Anforderungen 15 · Dokumentations- und Transparenzpflichten 13 · Zusammenspiel mit Datenschutz 9 · Sonstiges 4 · noch nicht relevant 2
Automatisierbare Tätigkeiten Top-3-Auswahl	Reporting 19 · Schulungsorganisation 16 · interne Untersuchungen 15 · Überwachung und Monitoring 14 · manuelle Datenerfassung 13 · Regulatory Monitoring 9 · Geschäftspartnerprüfung 8
Automatisierbare Prozesse	jährliches Risk Assessment 23 · Regulatory Monitoring 18 · Compliance-Reporting 16 · Schulungsmaterial 16 · Due Diligence 16 · Schulungsnachweise 16 · Geschenkeregister 15 · Policy Management 14 · Hinweisgeber-Meldungen 10 · KYC-Checks 10 · PEP-Screening 9 · interne Korrespondenz 6
Regulatorik-Tracking heute	manuelle Recherche 26 · Branchenverbände 20 · interne Rechtsabteilung 17 · externe Berater 16 · spezialisierte Tools 2
Wirksamkeitsmessung	nein 18 · ja 14
Gründe gegen Messung Basis: die 18	fehlende Datenbasis 15 · Messbarkeit weicher Faktoren 13 · kein geeignetes Tool 11 · Ressourcen und Zeit 8 · nie angefordert 7 · Sonstiges 1
Berichtsfrequenz Basis: die 14	jährlich 6 · quartalsweise 6 · halbjährlich 2
Erwartete Kernfunktionen	Reporting 29 · laufende Überwachung 24 · Risiko-Visualisierung 23 · Warnungen und Alarme 21 · Workflow-Automatisierung 20 · Dokumenten- und Policy-Verwaltung 18 · Audit-Unterstützung 12
Auslöser für Warnungen	KI-erkannte Anomalie 26 · fällige Fristen 23 · bestimmte Sachverhalte 22 · Schwellenwerte 19
Bevorzugte Visualisierung	Ampel-System 27 · Heatmap 20 · Trend-Linien 15 · Text-Zusammenfassung 10 · Geo-Map 8
Verfügbare Daten	unstrukturierte Dokumente 27 · E-Mails 22 · Excel-Listen 22 · strukturierte Datenbanken 18 · Log-Files 11 · weiss nicht 2
Anzubindende Systeme	ERP 20 · CRM 19 · Microsoft 365 19 · HR 16 · Finanzbuchhaltung 12 · GRC-Modul 10 · Legal-Tech 8 · Kernbankensystem 6
Integrationsart	vollautomatisch via API 15 · weiss nicht 5 · geplanter Batch-Import 5 · keine Präferenz 4 · manueller Upload 3
Verarbeitungsort	ausschliesslich intern 16 · hybrid 8 · externe Cloud akzeptabel 6 · keine Präferenz 2
Hosting	Private Cloud 11 · On-Premises 7 · weiss nicht 5 · SaaS 5 · keine Präferenz 4
Betriebsmodell	eigener Betrieb 13 · Betrieb durch Tool-Anbieter 9 · keine Präferenz 5 · weiss nicht 3 · Drittanbieter 2
Architektur	integrierte Plattform mit Modulen 16 · Best-of-Breed 7 · keine Präferenz 5 · weiss nicht 4
Zugang	eigenständiges Web-Dashboard 14 · in Teams/SharePoint 6 · weiss nicht 4 · in bestehendem GRC-Modul 4 · als PowerBI-Report 4
Rechtemodell	granular 21 · mandantenfähig 7 · einfach 4
Kontaktbereitschaft	ja 10 · nein 22 · E-Mail angegeben 11

ANHANG B

Quellen.

Alle Web-Abrufe am 21. August 2026, sofern nicht anders angegeben. [S] kennzeichnet Sekundärquellen ohne nachvollziehbare Methodik. Diese Angaben sind mit Vorbehalt zu lesen.

Primärdaten

1. MMIND.ai × Bratschi, AI Compliance Survey 2026, n=32, Erhebung 18.03.–31.05.2026.
2. MMIND.ai × Hanno Konrad Anstalt, Prototyp «Nachhaltigkeits-One-Pager für Bauprojekte», Projektpräsentation November 2025.
3. MMIND.ai, B Corp Eligibility Report für eine Treuhandgesellschaft in Vaduz, Stand 20.08.2026, auf Basis B Lab Standards V2.2 (20.02.2026).
4. MMIND.ai und KMU-HSG Universität St. Gallen, «Leitfaden Digitalisierung für KMU», 2025.

Regulatorik EU

1. Verordnung (EU) 2024/1689 (EU-AI-Act), insbesondere Art. 4, 25, 26, 50; EUR-Lex und AI Act Service Desk der Europäischen Kommission.
2. Gibson Dunn, «EU AI Act Omnibus Agreement: Postponed High-Risk Deadlines», zur politischen Einigung vom 06.05.2026. Veröffentlicht als Verordnung (EU) 2026/1744, ABl. L vom 24.07.2026, in Kraft seit 27.07.2026.
3. Latham & Watkins sowie Mayer Brown zu Art. 4 (KI-Kompetenz), gültig seit 02.02.2025.
4. Verordnung (EU) 2024/2847 (Cyber Resilience Act); Richtlinie (EU) 2024/1760 (CSDDD) samt Omnibus-Vereinfachungspaket 2025.
5. Lenz & Staehelin, zur extraterritorialen Wirkung des AI Act für schweizerische Unternehmen.

Regulatorik Schweiz und Liechtenstein

1. Bundesrat, «Positionspapier zur Regulierung von künstlicher Intelligenz», Medienmitteilung vom 12.02.2025.
2. EDÖB, «KI und Datenschutz», Stand 24.09.2025.
3. FINMA, Aufsichtsmitteilung 08/2024 vom 18.12.2024.
4. Datenschutzbeauftragte des Kantons Zürich, Merkblatt «Cloud-Produkte von US-Unternehmen», Februar 2026 (CLOUD Act).
5. Zum EWR-Stand des AI Act für Liechtenstein sowie zur KI-Strategie der Liechtensteinischen Landesverwaltung vom 14.04.2026 [S] , vor Publikation durch Regierungs- oder EFTA-Primärquelle zu ersetzen.

Sicherheit und Fehlerraten

1. Veracode, «2026 GenAI Code Security Report», 28.07.2026.
2. Cloud Security Alliance Labs, «AI-Generated Code Vulnerability Surge 2026», 04.04.2026, akt. 20.05.2026.
3. Cloud Security Alliance Labs, «Vibe Coding AI Governance Gap», 02.06.2026, enthält die IBM-Zahlen aus «Cost of a Data Breach 2025».
4. IANS Research, «Easy to Build, Easy to Expose», 15.05.2026.
5. Help Net Security, zu Prompt Injection als häufigster Ursache agentischer Sicherheitsvorfälle (OWASP), 11.06.2026.
6. The Hacker News, zum dokumentierten Repository-Upload durch eine CLI-Version, 14.07.2026.
7. Gravitee, «State of AI Agent Security 2026», n=919, berichtet über Sekundärquelle [S].

Halluzination und Produktivität

1. Magesh et al., Stanford RegLab, «Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools», 2024. Älteste Quelle im Papier, entsprechend einzuordnen.
2. Datenbank fabrizierter KI-Zitate in Gerichtsverfahren, Stand 09.06.2026 [S], Primärquelle Charlotin, HEC Paris.
3. METR, randomisierte kontrollierte Studie zur Entwicklerproduktivität mit KI-Unterstützung, 2025 (arXiv).

Werkzeuge und Datenresidenz

1. OpenAI, «Your data», Datenresidenz «Europe (EEA + Switzerland)», Herstellerdokumentation.
2. GitHub Changelog, «Copilot data residency in US, EU and FedRAMP», 13.04.2026, akt. 24.04.2026, EU Data Boundary inkl. EFTA seit 01.05.2026.
3. Mistral AI, Produkt- und Lizenzdokumentation zu Le Chat, Vibe CLI und offenen Gewichten.
4. Cursor, «Models and pricing», Herstellerdokumentation.
5. xAI/SpaceXAI, «Security FAQ», Herstellerdokumentation.
6. Moonshot AI, Modell- und Lizenzangaben zu Kimi K2.7 und K3 (Erstanbieter-Benchmarks, nicht mit SWE-bench Verified vergleichbar).
7. Anthropic, Produktdokumentation zu Skills, Cowork, Projects und Aufgaben.

Standards und Rahmenwerke

1. ISO 37301:2021, Compliance-Managementsysteme.
2. NIST AI Risk Management Framework (AI RMF 1.0).
3. U.S. DOJ, «Evaluation of Corporate Compliance Programs», Fassung September 2024.
4. B Lab, «Get started with the new standards», Stand 21.08.2026.

ANHANG C

Wie die Freitexte codiert wurden.

Vier Fragen waren offen gestellt: Pain Points (Frage 5), relevante Rechtsgebiete (7), verwendete Rahmenwerke (8) und Wunschfunktionen (24). Codierung ist Interpretation. Wir legen das Schema offen, damit die Zuordnung nachprüfbar bleibt.

KATEGORIE	REGEL	BEISPIEL AUS DEN ANTWORTEN
Daten, Werkzeuge und Reporting	Nennungen, die auf fehlende Datenbasis, untaugliche Systeme oder Aufwand in der Berichterstellung zielen	«Systeme, die technisch schwierig angepasst werden können, weshalb manuelle Arbeit hinzukommt»
Informationsflut und Regulatorik	Nennungen zu Menge, Tempo oder Mehrsprachigkeit regulatorischer Anforderungen	«Überflutung mit Informationen und Regeln»; «Überblick zu den aktuellen Anforderungen auch in anderen Rechtsräumen»
Aktualität von Weisungen	Nennungen zur Pflege, Aktualisierung und Durchdringung eigener Regelwerke	«Aktualisierung Manuals/Reglemente an aktuelle Entwicklungen im Compliancebereich»
Kultur und Integration	Nennungen zur Verankerung der Funktion im Unternehmen, inklusive negativer Selbstbeschreibungen	«zu wenig integriert – viele losgelöste Aktionen, aber fehlendes Gesamtbild»; «leider zu oft noch ein notwendiges Übel»
Aufwand für Einzelfälle	Nennungen zum Aufwand für Untersuchungen, Abklärungen und Falschtreffer	«Bei Compliance-Filtern zu viele false positive Treffer, die manuell abgearbeitet werden müssen»
Schulung und Nachweis	Nennungen zu Schulungsorganisation, Nachweisen und Zielgruppenzuschnitt	«Schulungen und Schulungsnachweise zu zwingenden Compliance-Themen»

Hinweise zur Redlichkeit

- **Mehrfachzuordnung ist möglich.** Eine Antwort, die mehrere Themen anspricht, wurde mehreren Kategorien zugeordnet. Die Summe der Kategorien übersteigt deshalb die Anzahl Antworten.
- **Leere und Platzhalterantworten** wie «keine», «n/a» oder «–» wurden nicht codiert, sondern als fehlend behandelt und in der jeweiligen Basis nicht mitgezählt.
- **Zwei Antworten zur Wirksamkeitsmessung** nannten Gründe gegen eine Messung, obwohl sie die Frage mit «Ja» beantwortet hatten. Wir haben die Gründe ausschliesslich auf die Basis der 18 «Nein»-Antworten bezogen; die Rohsumme über alle 32 wäre bei einzelnen Gründen um eins höher.

Kontakt

mmind.ai

Hartmut Hübner

Co-Founder

hartmut@mmind.ai
MMIND GmbH
Duxgass 55
9494 Schaan
Liechtenstein

bratschi

Christian Wind

Partner

christian.wind@bratschi.ch
Bratschi AG
Bahnhofstrasse 70
P.O. Box
CH-8021 Zürich

© 2026 MMIND GmbH und Bratschi AG. Keine Rechtsberatung. Stand 21. August 2026.