BVMW-IMPULS · MONTAG, 8. JUNI 2026

KI-Agenten, Vibe Coding und der EU AI Act

Wir bauen live einen Prüfkatalog für den KI-Einsatz und halten an jeder Entscheidung an, die zählt.

Dr. Oliver Gausmann

Geschäftsführer Convios · KI-Strategie und Governance

WER UND WAS

Kurz zu mir, und was wir gleich tun

Dr. Oliver Gausmann

Convios. Ich begleite Mittelständler bei KI-Strategie und Governance, oft in regulierten Branchen. 20+ Jahre operativ in Konzern, im Mittelstand und im Startup.
Lehrauftrag Softwaremanagement Uni Zürich.

Die nächsten 30 Minuten

Wir bauen live eine kleine Anwendung, einen Prüfkatalog für den KI-Einsatz. An sechs Stellen halten wir an, wo eine echte Entscheidung fällt, und ordnen sie rechtlich ein.

Ein Prüfkatalog taugt nur, wenn man ihn individuell befüllen kann.
Wir bauen diese Anwendung hier zusammen.

WARUM ÜBERHAUPT REGELN

Erst die Checkliste macht das Tempo möglich

Als Pilot wird ein Flug durch Checklisten, Instrumente und klare Verfahren sicher. Erst das macht Fliegen schnell, weit und alltäglich.

Mit KI ist es genauso. Das Potenzial ist enorm, das Risiko real. Die Regeln sind die Checkliste, die das Potenzial nutzbar macht.

Und genau diese Checkliste bauen wir jetzt.

Vor dem Start

- Potenzial benennen
- Risiko kennen
- Verfahren festlegen

BEGRIFF 1 · VIBE CODING

Software per Sprache beschrieben

Sie beschreiben in normaler Sprache, was die Software tun soll. Die KI schreibt den Code. Aus einem Satz wird eine lauffähige Anwendung.

2023

Autovervollständigung

Die KI ergänzt einzelne Zeilen.

2024

Chat-Assistent

Sie schreibt Funktionen auf Zuruf.

2026

Agentischer Builder

Sie baut und deployt ganze Apps.

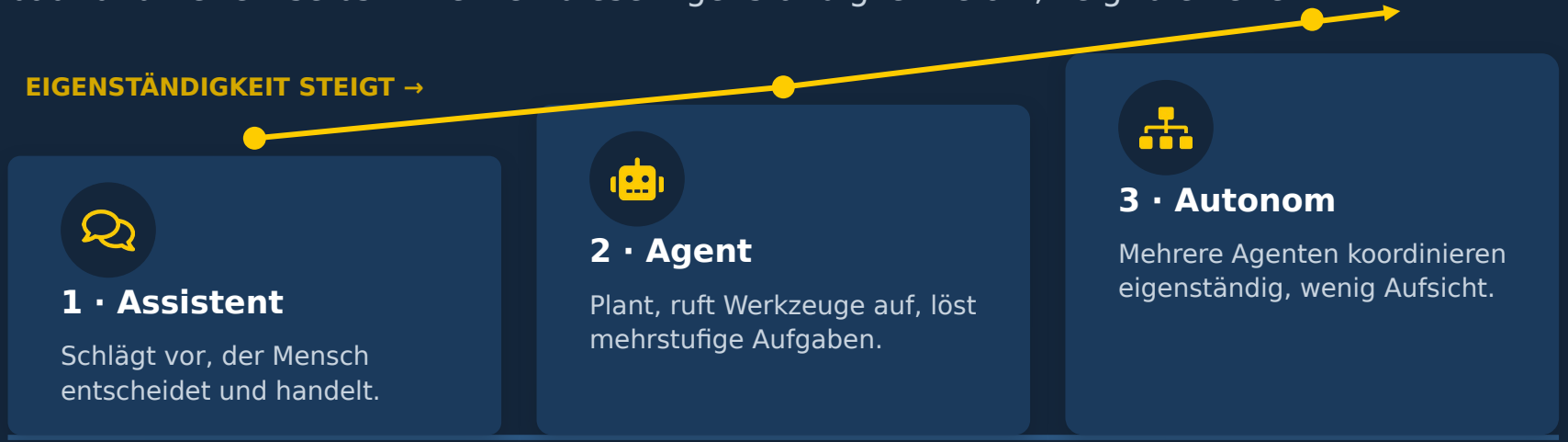
Die Kehrseite: Rund 45 Prozent des KI-Codes hat bekannte Sicherheitslücken; ein CMU-Benchmark wertet sogar nur 10,5 Prozent des funktionierenden Codes als sicher. Der neue Job dazu heißt Vibe Code Cleanup Specialist. **Schöner ist, ihn gar nicht erst zu brauchen.**

Veracode, GenAI Code Security Report 2025 · SUSVIBES, Zhao u. a. (CMU) 2026 · neue LinkedIn-Rolle seit 2025

BEGRIFF 2 · KI-AGENTEN

Vom Prompt zum Agenten

Vibe Coding: der Mensch promptet, die KI schreibt. **Agentic Engineering:** die KI plant, baut und iteriert selbst. Wie weit diese Eigenständigkeit reicht, zeigt die Leiter.



Je höher die Stufe, desto mehr **Aufsicht, Protokoll und Not-Aus**. Die Verantwortung bleibt im Haus.

KI-MENSCH-AUGMENTATION

Centaur, Cyborg, Self-Automator

Drei Arten, mit KI zu arbeiten.

14 %

Centaur

Gezielte Zusammenarbeit

Klare, eng geführte Fragen. Sie behalten das Urteil.

Höchste Treffsicherheit, baut Fachwissen auf.
WANN: wichtige Entscheidungen

60 %

Cyborg

Enge Verzahnung

Ständiges Hin und Her mit der KI an einer Aufgabe.

Lernt das KI-Handwerk, weniger Fachtiefe.
WANN: kreatives, exploratives Arbeiten

27 %

Self-Automator

Volle Abgabe

Aufgabe ganz an die KI abgegeben, kaum Prüfung.

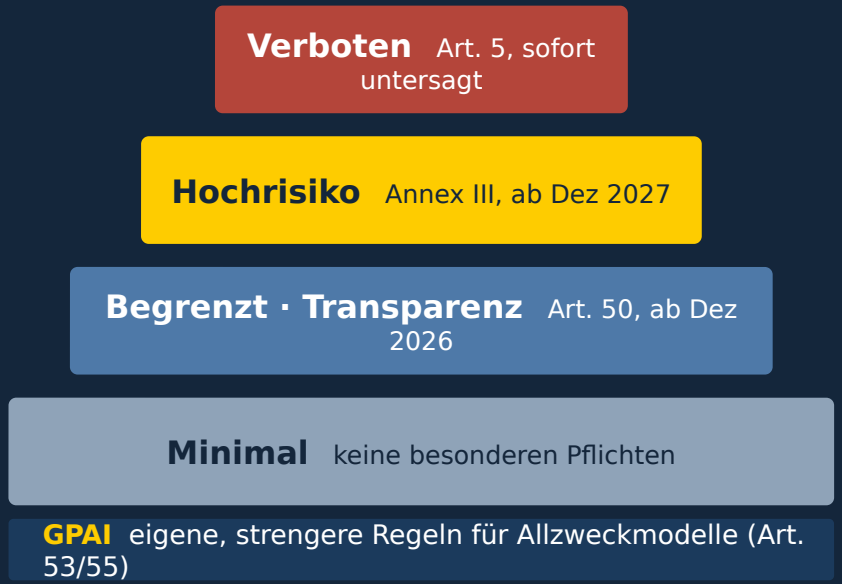
Schnell, aber flach. Kein Kompetenzgewinn.
WANN: nur Routine mit geringem Risiko

Den Modus pro Aufgabe wählen: Wichtiges als **Centaur**, Kreatives als **Cyborg**, Routine als **Self-Automator**. Je höher das Risiko, desto mehr Mensch.

Studie: Kellogg, Lifshitz, Dell'Acqua, Mollick u. a. (MIT Sloan / HBS, 2024), 244 Berater

BEGRIFF 3 · EU AI ACT

Nach Risiko reguliert, mit klaren Fristen



Faustregel: im Zweifel höher einstufen und nachfragen.

WAS WANN GILT

- **seit Feb 2025** Schulungspflicht (Art. 4), Verbote (Art. 5)
- **seit Aug 2025** GPAI-Pflichten und Bußgelder (Art. 53/99)
- **ab Dez 2026** Kennzeichnung KI-erzeugter Inhalte (Art. 50)
- **ab Dez 2027** Hochrisiko (Annex III) samt Betreiberpflichten

Annex I in regulierten Produkten ab Aug 2028. Omnibus politisch geeinigt am 7. Mai 2026, formale Verabschiedung offen. Bis dahin bleibt der 2. August 2026 rechtlich aktiv.

DAS REGELWERK UM KI

Der AI Act steht nicht allein

DSGVO

Immer, sobald personenbezogene Daten im Spiel sind. Grundlage (Art. 6), Vertrag (Art. 28), Speicherort.

NIS2

In Kraft seit Dez 2025. Ab 50 MA oder 10 Mio € Umsatz. Die Geschäftsführung haftet persönlich (§ 38).

Produkthaftung neu

Ab Dez 2026 gilt Software als Produkt. Haftung ohne Verschuldensnachweis.

Urheberrecht

Training und Wiedergabe geschützter Werke verletzen das Recht. Der Anbieter haftet. LG München, 11.11.2025.

JETZT BAUEN WIR

Sechsmal halten wir an

BEVOR WIR BAUEN

1 · Business Case

2 · Befugnis & Fähigkeit

WÄHREND WIR BAUEN

3 · Werkzeug & Tarif

4 · Daten & Input/Output

5 · Hosting

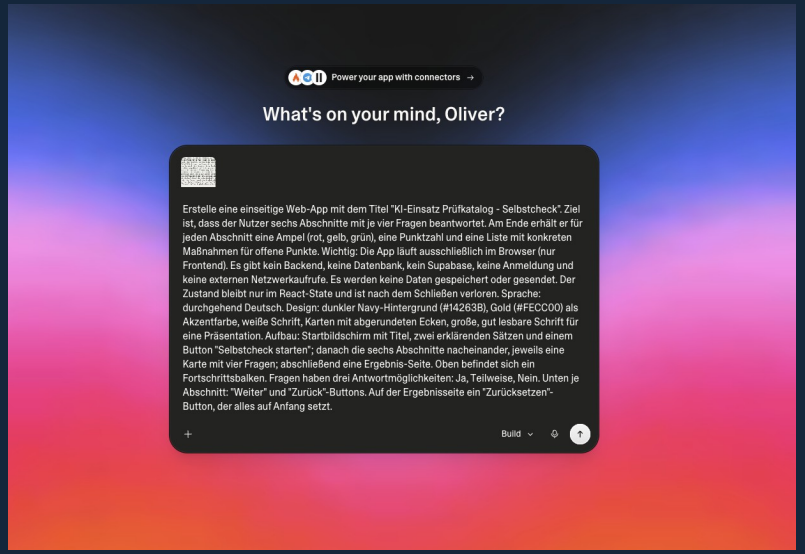
NACHDEM ES LÄUFT

6 · Betrieb & Lebenszyklus

Werkzeug heute: **Lovable** (Cloud, EU-gehostet in Stockholm).

Will ich das überhaupt selbst bauen?

Die erste Prüfung ist die Wirtschaftlichkeit, keine Rechtsfrage.



SIE ENTSCHEIDEN

Selbst bauen nur, wenn es das nicht von der Stange gibt und sich rechnet. Sonst kaufen.

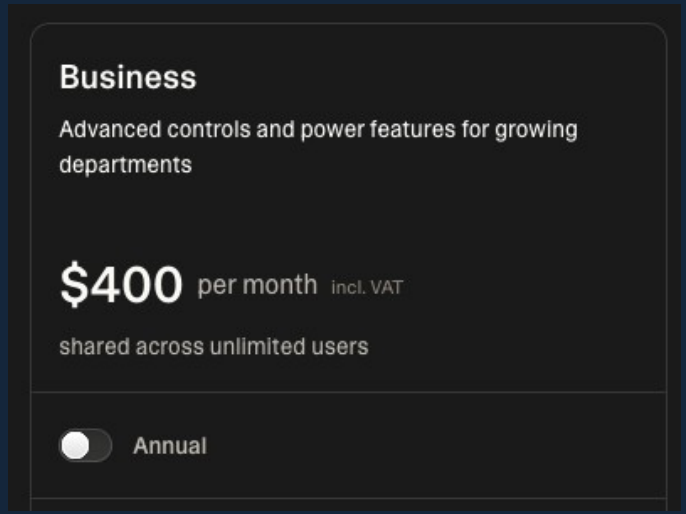
WIRTSCHAFTLICHKEIT ZUERST

Kostenfalle: Der Bau ist nur 20–30 % der Gesamtkosten. Mehr im Anhang.

BEVOR | WÄHREND | DANACH

Darf und kann diese Einheit das bauen?

Kompetenz samt rechtlicher Einschätzung, plus Freigabe durch die IT-Governance.



SIE ENTSCHEIDEN

Bauen mit Freigabe und vorhandener Kompetenz. Ohne Freigabe ist es selbst gemachte Schatten-KI.

EU AI ACT · ART. 4 | IT-GOVERNANCE | ISO/IEC 42001

Für den GF: Kompetenz nachweisen (Art. 4), ISO 42001 als Rahmen.

Welches Tool, welcher Plan?

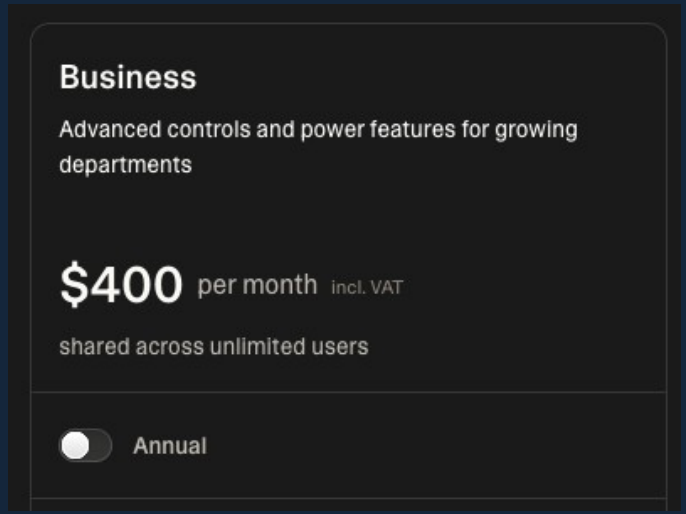
Tarif, Vertrag, Standort und Anbieter entscheiden über Rechtskonformität.

SIE ENTSCHEIDEN

Business-Tarif mit Auftragsverarbeitung (AVV), Training aus. Lovable liegt in der EU, ein echter Pluspunkt.

DSGVO · ART. 28 (AVV)

STANDORT & ANBIETER



Lovable Auftragsverarbeitungsvertrag

Welche Daten, und speichert die App etwas?

Echte personenbezogene Daten nur mit Rechtsgrundlage und Vertrag.

SIE ENTSCHEIDEN

Client-only: der Selbstcheck rechnet im Browser, nichts wird gespeichert. Lovables Default-Datenbank bleibt aus.

DSGVO · ART. 5/6/28

INPUT / OUTPUT

2025: 170+ Lovable-Apps offen durch ungeschützte Default-DB (CVE-2025-48757).

LIVE: SPRUNG IN DIE APP

KURZ ERKLÄRT

Der Selbstcheck rechnet vollständig im Browser. Der Netzwerk-Tab bleibt leer: keine Daten verlassen das Gerät, nichts wird gespeichert.

Wo läuft das, wo stehen die Daten?

Statisch ohne Backend ist unkompliziert. Mit Server zählen Standort und Absicherung.

SIE ENTSCHEIDEN

Veröffentlichen auf lovable.app, dann Export nach GitHub. Der Code gehört Ihnen.

DSGVO · SPEICHERORT **SECURITY**

Optionen: SQL (Postgres), NoSQL, Datei/Storage. Git ist keine DB. Anhang.

LIVE: SPRUNG IN DIE APP

KURZ ERKLÄRT

Veröffentlichung auf lovable.app, danach Export nach GitHub. Der Code gehört dem Unternehmen und bleibt unabhängig vom Werkzeug betreibbar.

Wer besitzt, wartet und beendet die App?

Je schneller die KI baut, desto mehr fällt von der eingebauten Prüfung weg.

SIE ENTSCHEIDEN

Owner benennen, Sicherheits-Patches planen, regelmäßiger KI-Security-Lauf, klares Ende festlegen.

PRODUKTHAFTUNG 2026

NIS2 · ROLLEN

LIVE: SPRUNG IN DEN REPORT

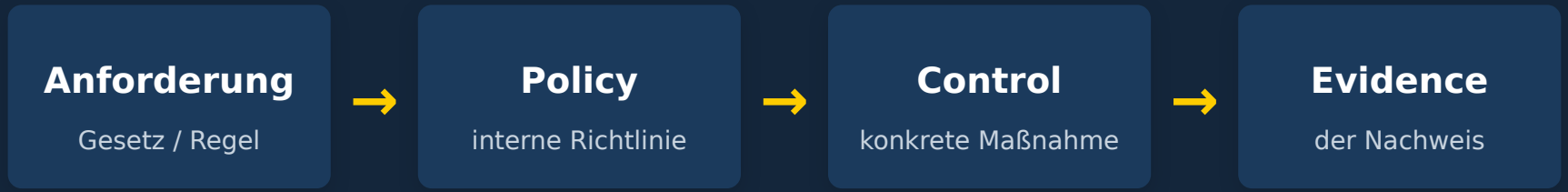
SECURITY SELF-ASSESSMENT

Gesamtbewertung: GRÜN

Methodik: STRIDE · OWASP Top 10
Client-only, kein Backend, keine Daten.
Offen: CSP-Header, Dependency-Scan, Hosting-Region.

DER ROTE FADEN

Aus jeder Entscheidung wird ein Nachweis



Lücke = Risiko. Fehlt der Nachweis, entsteht es automatisch.

Die sechs Punkte sind die Abschnitte des Katalogs. **Jeder verlangt einen Nachweis, kein Bauchgefühl.**

Verankert in EU AI Act Art. 12 (Protokollierung) und Art. 26 (Aufbewahrung) sowie DSGVO Art. 5 Abs. 2 (Rechenschaftspflicht).

FAZIT

Der Prüfkatalog steht

Und er ist genau die Liste, die wir gerade gebaut haben. Eine App in zwei Stunden bauen kann heute fast jeder. Sie verantwortbar zu betreiben ist die eigentliche Leistung.

Ihr nächster Schritt: Den Prüfkatalog und das Repo als Lehrbeispiel gibt es zum Mitnehmen. Verbinden Sie sich auf LinkedIn oder schreiben Sie mir.

Ihre Fragen.

Dr. Oliver Gausmann

Geschäftsführer Convios GmbH

KI-Strategie · KI-Governance · EU AI Act

LinkedIn: Dr. Oliver Gausmann

olivergausmann.com

convios.com

Auf LinkedIn vernetzen

FALLS GEFRAGT · WELCHER PLAN

Consumer oder Unternehmen

Consumer-Tarif

Free, Pro, Plus, Max. Training per Default an, lange Speicherung, kein Vertrag. Für echte Firmendaten ungeeignet.

Beispiele: ChatGPT Plus, Claude Pro

Business / Enterprise / API

Kein Training mit Ihren Daten, kurze Speicherung, Vertrag verfügbar, oft EU-Region wählbar. Der richtige Weg fürs Unternehmen.

Gilt für Claude Code, Codex, Lovable & Co.

Der Tarif ist der erste Filter, nicht der einzige.

FALLS GEFRAGT · TOOL-WAHL

Mehr als der Tarif

Tarif & Training

Business, Enterprise oder API. Kein Training mit Ihren Daten, kurze Speicherung.

Vertrag

Auftragsverarbeitung nach DSGVO Art. 28. Ohne Vertrag keine Firmendaten.

Standort

Wo steht das Rechenzentrum? EU-Region wählbar? Wer hat Zugriff?

Anbieter

Trägt er wirtschaftlich? Viele KI-Anbieter sind jung, manche werden übernommen oder verschwinden.

Die Marke entscheidet wenig. Tarif, Vertrag, Standort und Bestand des Anbieters entscheiden.

QUELLEN

Definitionen und Belege

RECHT & REGULIERUNG

EU AI Act, VO (EU) 2024/1689
eur-lex.europa.eu/eli/reg/2024/1689/oj

AI-Omnibus, Einigung 7. Mai 2026
Rat der EU; Analyse: hoganlovells.com

DSGVO, VO (EU) 2016/679
eur-lex.europa.eu/eli/reg/2016/679/oj

NIS2-RL (EU) 2022/2555; NIS2UmsuCG, BSIG
bsi.bund.de

Produkthaftung, RL (EU) 2024/2853
eur-lex.europa.eu/eli/dir/2024/2853/oj

LG München I, 11.11.2025, 42 O 14139/24
justiz.bayern.de

KONZEPTE & DATEN

Vibe Coding zu Agentic Engineering: GLM-5, 2026
arxiv.org/abs/2602.15763

Drei Modi (Centaur/Cyborg/Self-Automator): Kellogg, Lifshitz, Dell'Acqua, Mollick u. a., 2024
mitsloan.mit.edu · SSRN 4921696

Vibe Coding (Begriff): Karpathy 2025; Collins WotY 2025
collinsdictionary.com

KI-Code-Sicherheit, 45 %: Veracode 2025
veracode.com

Vibe Security Radar, 35 CVEs März 2026: Georgia Tech
scp.cc.gatech.edu

Vibe-Coding-Sicherheit, SUSVIBES: Zhao u. a. (CMU) 2026
arxiv.org/abs/2512.03262

Risikoklassen im Detail

Inakzeptabel — verboten Unvertretbare Gefahr: Manipulation, Grundrechtsverletzung, Schaden.
z. B. staatliches Social Scoring, biometrische Echtzeit-Überwachung, Ausnutzen von Schwächen (Kinder)

Hoch — streng reguliert Erhebliche Wirkung auf Gesundheit, Sicherheit, Grundrechte. Konformitätsbewertung vor Nutzung.
z. B. KI in Medizinprodukten, Personalauswahl, Bonitätsprüfung, kritische Infrastruktur

Begrenzt — Transparenzpflicht Aufklärungspflicht beim Kontakt mit KI oder KI-Inhalten.
z. B. Chatbots, Deepfakes — Nutzer müssen erkennen, dass KI im Spiel ist

Minimal — nahezu unreguliert Kein signifikantes Risiko; freiwillige Verhaltenskodizes empfohlen.
z. B. Spamfilter, Spielgegner-KI

GPAI eigene, strengere Regeln für mächtige Allzweckmodelle (Art. 53/55)

Mitnehmsatz: Vor jeder KI-Aufgabe die Risikoklasse klären, im Zweifel höher einstufen. Das gehört geschult.

Was KI wirklich kostet

ECHTE KOSTENTREIBER

- Daten: sammeln, bereinigen, schützen (30–50 % des Budgets)
- Inferenz/Token: bei Agenten 80–90 % der laufenden Kosten
- Integration in bestehende Systeme und Prozesse
- Sicherheit, Datenschutz, Compliance, Audits
- Betrieb: Monitoring, Updates, Skalierung
- Personal: Betreuung, Weiterentwicklung

FAUSTZAHLEN

2–4×
Gesamtkosten gegenüber dem Listenpreis

20–30 %
Anteil der Lizenz an den Gesamtkosten

20–40 %
jährliche Wartung des Erstinvests

Beispiel: Eine 200-€-Vibe-App vs. ein produktives System mit Datenbank, Nutzern und Anbindung — schnell sechsstellig pro Jahr.

Quellen: TCO-Analysen Enterprise AI 2025 (u. a. Xenoss, Glean, StackAI); Inferenzanteil agentischer Systeme.

Datenbanken im Überblick

Relational / SQL Tabellen mit festen Beziehungen, sehr verbreitet.	*PostgreSQL, MySQL, MariaDB*
Dokument / NoSQL Flexible Datensätze ohne festes Schema.	*MongoDB, CouchDB*
Key-Value / Cache Sehr schnelle Schlüssel-Wert-Speicher.	*Redis*
Datei- / Objekt-Speicher Für Dateien, Bilder, Backups.	*Amazon S3, Azure Blob*
Backend-as-a-Service Datenbank plus Auth fertig gebündelt (Lovable-Default).	*Supabase, Firebase*

Git ist keine Datenbank — es ist Versionsverwaltung für Code (Stand, Historie, Rückrollen).

Mitnehmsatz: Sobald eine Datenbank Personendaten hält, braucht sie Zugriffsschutz (RLS) — sonst droht der Lovable-Fall.

ANHANG · AUSBLICK

Die agentische Organisation

KI-Agenten übernehmen zunehmend Entscheidungen und ganze Abläufe. Ein Agent arbeitet im Zyklus Denken, Planen, Handeln, Reflektieren — Teams aus Agenten koordinieren sich, oft mit einem Guardian-Agenten als Aufseher.

WAS DAS FÜR DIE GESCHÄFTSFÜHRUNG HEISST

→ **Von Befehl und Kontrolle zu Koordination und Aufsicht**
Sie steuern nicht mehr jeden Schritt, sondern richten Agenten und Teams aus und überwachen Ergebnisse.

→ **Eigene KI-Kompetenz aufbauen**
Führung muss Fähigkeiten und Grenzen der Agenten einschätzen können, um Ergebnisse zu beurteilen.

→ **Systemische Risiken und Not-Aus einplanen**
Regelmäßige Audits, Fail-Safes und ein menschlicher Eingriff für den Ernstfall.

→ **Ethik, Rechenschaft und Governance**
Verhalten der Agenten überwachen, Verantwortung klar zuordnen, Nachweise führen.

Quelle: Gassmann, Wincent, „The Non-Human Enterprise: How AI Agents Reshape Organizations“, California Management Review, 22.10.2025.