

## KI-Weisung für Verwaltungsräte und Mandatsfirmen

Klare Guardrails für verantwortungsvollen KI-Einsatz, strategische Kontrolle und wirksame Aufsicht.

|                |                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable</b>  | KI wird dort genutzt, wo sie Recherche, Entwurf, Strukturierung, Qualitätssicherung und Administration messbar verbessert.   |
| <b>Protect</b> | Mandatsdaten, Board-Unterlagen, Personendaten, Berufsgeheimnisse und strategische Informationen bleiben geschützt.           |
| <b>Prove</b>   | Wesentliche KI-Nutzungen werden mit Tool, Zweck, Datenzone, Kontrolle und menschlicher Prüfung nachvollziehbar dokumentiert. |

### Muster für BoardCompliance AG / BoardPlus Kontext

Showcase-Kontext: Dr. Leonz Meyer, BoardCompliance AG / BoardPlus

Homepage Edition | Juni 2026 | Sallenbach AG | AI & Innovation Consulting | [www.sallenbach.org](http://www.sallenbach.org) | [vero@sallenbach.org](mailto:vero@sallenbach.org)

# Wozu diese Weisung dient

Sie ist als pragmatischer Startpunkt geschrieben: Boards können sie an Mandatsfirmen weiterleiten, Geschäftsleitungen können daraus interne Regeln ableiten, und Teams erhalten klare Leitplanken für die tägliche KI-Nutzung.

Hinweis für Leonz / BoardCompliance: Für anwaltliche Mandatsarbeit, Board-Unterlagen und Konsulatskommunikation gilt erhöhte Vorsicht. Öffentliche Chatbots sind für solche Daten nicht geeignet; zulässig sind nur explizit freigegebene und vertraglich geprüfte Umgebungen.

# Text an die Belegschaft

Liebe Mitarbeitende

Künstliche Intelligenz ist inzwischen Teil unseres Arbeitsalltags: in E-Mails, Office-Tools, Recherche, Präsentationen, Protokollen, Datenanalyse und zunehmend auch in automatisierten Workflows. Wir möchten diese Möglichkeiten nutzen, aber mit klaren Leitplanken.

Diese KI-Weisung beschreibt, welche Daten in welche Tools eingegeben werden dürfen, wann eine Freigabe erforderlich ist, wie KI-Ergebnisse geprüft werden und wie Unsicherheiten oder Vorfälle gemeldet werden.

Bitte nutzt KI pragmatisch, aber bewusst: keine vertraulichen, personenbezogenen, mandatsbezogenen, marktpreisrelevanten oder geschützten Informationen in nicht freigegebene öffentliche KI-Tools eingeben; Outputs kritisch prüfen; Quellen sichern; Unsicherheiten früh melden.

Die Weisung ist als Startpunkt gedacht. Fragen, Tool-Vorschläge oder Unsicherheiten können an die zuständige Person für KI, Datenschutz, Legal oder Compliance gerichtet werden.

Beste Grüße

[Verwaltungsrat / Geschäftsleitung]

# Datenzonen-Kompass

Die Zonen übersetzen abstrakte Datenschutz- und Geheimhaltungspflichten in eine einfache Arbeitsregel: Erst Datenzone bestimmen, dann Tool wählen.

| Zone                                      | Datenbeispiele                                                                                              | Regel                                                                                                    |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Grün: Öffentlich</b>                   | Öffentliche Informationen, Website-Texte, bereits veröffentlichte Inhalte, allgemeine Ideen.                | Öffentliche KI-Tools sind möglich, sofern keine verdeckten vertraulichen Informationen im Prompt stehen. |
| <b>Gelb: Intern</b>                       | Interne, nicht vertrauliche Arbeitsentwürfe, anonymisierte Beispiele, allgemeine Prozessideen.              | Nur freigegebene Business- oder Enterprise-Tools; keine unnötigen Personen- oder Kundendaten.            |
| <b>Orange: Sensibel</b>                   | Personendaten, HR, Kundenlisten, interne Finanzaufzeichnungen, nicht veröffentlichte Management-Unterlagen. | Nur geprüfte Tools mit geklärter Datenhaltung, Rollen, Löschung, Vertrag und Zugriffskontrolle.          |
| <b>Rot: Vertraulich / Berufsgeheimnis</b> | Mandatsdaten, Rechtsfragen, Board-Unterlagen, M&A, Krise, Konsults- und Kundendaten.                        | Keine öffentlichen Tools. Nutzung nur in explizit freigegebenen, sicheren Legal-/Enterprise-Umgebungen.  |
| <b>Schwarz: Höchstschutz</b>              | Insiderinformationen, Streitigkeiten, Untersuchungen, hochsensible Strategie- oder Transaktionsdaten.       | KI-Nutzung nur nach Einzelentscheid von Legal/Compliance/Board und mit dokumentiertem Schutzkonzept.     |

# 1. Zweck und Geltungsbereich

Diese Muster-KI-Weisung regelt den verantwortungsvollen Einsatz von künstlicher Intelligenz in Unternehmen, die durch einen Verwaltungsrat, Aufsichtsrat oder ein vergleichbares Board überwacht werden. Sie richtet sich an Board-Mitglieder, Geschäftsleitung, Mitarbeitende, externe Beratende, Freelancer und weitere Personen, die im Auftrag des Unternehmens mit KI-Systemen arbeiten.

Ziel ist, KI-Nutzung zu ermöglichen, ohne Vertraulichkeit, Datenschutz, Geschäftsgeheimnisse, Berufsgeheimnisse, Urheberrechte, Reputation, Entscheidungsqualität oder regulatorische Pflichten zu gefährden.

Für BoardCompliance / BoardPlus gilt als zusätzlicher Praxisanker: Mandatsdaten, VR-Unterlagen, anwaltliche Einschätzungen, Konsultatskommunikation und Kundenfragen sind grundsätzlich erhöht schutzbedürftig und dürfen nicht in öffentliche KI-Tools eingegeben werden.

## 2. Board-Prinzipien

Verantwortung bleibt menschlich: KI unterstützt Analyse, Entwurf, Strukturierung und Qualitätssicherung. Entscheidungen des Boards, der Ausschüsse und der Geschäftsleitung werden nicht an KI delegiert.

Vertraulichkeit zuerst: Vertrauliche Board-Unterlagen, Strategie-, Finanz-, HR-, M&A-, Rechts- und Kundendaten dürfen nur in freigegebenen, vertraglich geprüften Umgebungen verarbeitet werden.

Wertschöpfung vor Hype: KI wird dort eingesetzt, wo sie bessere Vorbereitung, schnellere Orientierung, höhere Qualität oder robustere Kontrollen ermöglicht.

Transparenz und Nachvollziehbarkeit: Wesentliche KI-Nutzungen werden dokumentiert: Tool, Zweck, Datenklasse, verantwortliche Person, Freigabe und Kontrollschritte.

Security und Datenschutz by Design: Neue KI-Anwendungen werden vor Einsatz auf Datenflüsse, Hosting, Training, Human Review, Zugriff, Protokollierung, Löschung und Exit geprüft.

## 3. Rollen und Verantwortlichkeiten

Verwaltungsrat / Aufsichtsrat: genehmigt Grundsätze, Risikobereitschaft, wesentliche KI-Vorhaben und jährliche Berichterstattung. Er verlangt ein KI-Register und überprüft kritische Use Cases.

Ausschüsse: prüfen die für ihren Auftrag relevanten KI-Risiken. Audit, Risk und Compliance achten besonders auf Kontrollen, Datenschutz, Informationssicherheit und Berichtsqualität.

Geschäftsleitung: setzt die Weisung um, benennt Verantwortliche, führt Tool- und Use-Case-Register und stellt Schulung sowie Kontrollen sicher.

KI-Verantwortliche/r: prüft Tools, koordiniert Freigaben, dokumentiert Risiken und betreut Incident Response.

Nutzende und externe Mitwirkende: halten Datenzonen und Freigaben ein, prüfen Resultate kritisch und melden Fehlverhalten, Datenabfluss oder kritische Outputs sofort.

## 4. Erlaubte Board-Use-Cases

Board-Briefings: Zusammenfassung regulatorischer, technologischer oder marktbezogener Entwicklungen. Quellen prüfen; keine vertraulichen Inputs in nicht freigegebene Tools.

Sitzungsvorbereitung: Agendaentwurf, Fragenkatalog, Risikomatrix und Entscheidungsoptionen. Finale Unterlagen durch verantwortliche Person freigeben.

Policy- und Reglementsentwürfe: Erste Fassungen für KI-Weisung, Datenschutz, Informationssicherheit, Delegationsordnung oder Playbooks. Juristische Prüfung bleibt zwingend.

Risikoregister und Kontrollfragen: Identifikation von Schwachstellen, Massnahmen und Monitoring-Fragen. Risiken priorisieren und im Board-Protokoll nachvollziehbar festhalten.

Training, AI Avatare und Simulation: Board-Szenarien zu Cyber, Krise, Medien, Haftung, EU AI Act oder Datenschutz. AI Avatare müssen als solche erkennbar sein; Bild-, Stimm- und Skriptrechte sind zu klären.

## 5. Unzulässige oder besonders freigabepflichtige Nutzung

Keine Eingabe vertraulicher, personenbezogener, mandatsbezogener, marktpreisrelevanter oder berufsgeheimer Informationen in nicht freigegebene öffentliche KI-Tools.

Keine automatisierte Entscheidung über Personal, Vergütung, Bonität, Kredit, Versicherung, Leistung, Kündigung oder Zugang zu Dienstleistungen ohne gesonderte rechtliche Prüfung.

Keine verdeckte Transkription, Aufzeichnung oder Analyse von Board-Sitzungen ohne vorgängige Information, Rechtsgrundlage, Tool-Freigabe und klare Löschfristen.

Keine Veröffentlichung von KI-generierten Aussagen, Zahlen, Rechtsbehauptungen, Finanzinformationen oder Avatar-Videos ohne unabhängige Prüfung und Freigabe.

Keine autonome Kommunikation von KI-Agenten an Kunden, Behörden, Investoren oder Medien ohne definierte Freigabegrenzen und menschliche Endkontrolle.

## 6. Tool-Freigabe und KI-Register

Vor dem produktiven Einsatz eines KI-Tools ist eine Freigabe erforderlich. Das Board verlangt mindestens ein schlankes KI-Register, das jährlich oder bei wesentlichen Änderungen überprüft wird.

Das Register dokumentiert Zweck, Use Case, Tool, Datenzone, verantwortliche Person, Datenflüsse, Hosting, Training/Human Review durch Provider, Zugriff, Löschung, Kontrollen und Status.

Besonders zu prüfen sind: Zero Data Retention, No Human Review, Subprozessoren, Drittlandtransfer, CLOUD-Act-Risiken, Rollenrechte, Protokollierung, Vertragsgrundlagen und Exit-Möglichkeiten.

## 7. Qualitätssicherung und Human-in-the-loop

KI-Outputs sind Arbeitsentwürfe. Wer KI nutzt, bleibt für Richtigkeit, Vollständigkeit, Aktualität, Angemessenheit, Tonalität und rechtliche Tragfähigkeit verantwortlich.

Fakten, Zahlen, Zitate, Rechtsaussagen und Quellen werden unabhängig geprüft. Bei rechtlichen, finanziellen, regulatorischen oder reputationsrelevanten Themen erfolgt eine qualifizierte Zweitprüfung.

Entscheidungsunterlagen für das Board enthalten keine ungeprüften KI-Behauptungen. Wesentliche Annahmen, Unsicherheiten und Datenlücken werden transparent gemacht.

## 8. Board-Sitzungen, Protokolle und vertrauliche Räume

Für Sitzungen des Boards gelten erhöhte Anforderungen. KI-gestützte Transkription, Zusammenfassung, Übersetzung oder Analyse ist nur zulässig, wenn Zweck, Teilnehmerinformation, Tool-Freigabe, Datenhaltung, Löschung und Zugriff klar geregelt sind.

Board-Regel: Keine KI-Aufzeichnung von Sitzungen ohne vorherige Information und definierte Löscho- oder Aufbewahrungslogik. Für Krisen-, M&A-, Personal-, Rechts- und Insider-Themen gilt grundsätzlich Zone Rot oder Schwarz.

## 9. Agentische Workflows und Automatisierung

KI-Agenten, die selbständig recherchieren, E-Mails vorbereiten, Daten abfragen, Termine buchen, Dokumente verändern oder externe Systeme auslösen, benötigen eine separate Freigabe.

Agenten erhalten nur die minimal erforderlichen Rechte. Externe Kommunikation, Zahlungen, Vertragsänderungen und Datenexporte benötigen menschliche Bestätigung.

Aktionen, Eingaben, Ausgaben und Freigaben müssen nachvollziehbar sein. Verantwortliche können den Agenten jederzeit deaktivieren. Neue Agenten werden zuerst mit Testdaten, begrenztem Scope und klaren Erfolgskriterien geprüft.

## 10. Incident Response

Jede Person meldet unverzüglich, wenn vertrauliche Daten in ein falsches Tool eingegeben wurden, ein KI-System unbefugt Zugriff erhalten hat, ein kritischer Fehloutput verwendet wurde oder Anzeichen für Datenabfluss, Manipulation, Bias oder Sicherheitsverletzungen bestehen.

Sofortmassnahmen: Nutzung stoppen, Veröffentlichung oder Agenten-Aktion anhalten, Zeitpunkt, Tool, Prompt, Output, betroffene Daten und beteiligte Personen dokumentieren und KI-Verantwortliche/r, Legal, Datenschutz, IT-Security sowie bei Bedarf Board-Präsidium informieren.

# Board Quick Check

Zwölf Fragen für die nächste Board- oder Geschäftsleitungssitzung.

| #  | Kontrollfrage                                                                                         | Status                                                                                       |
|----|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| 1  | Gibt es eine verabschiedete KI-Weisung und ist sie allen relevanten Personen bekannt?                 | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 2  | Sind Datenzonen definiert, insbesondere für Board-, Mandats-, HR-, Finanz- und Kundendaten?           | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 3  | Gibt es eine Liste erlaubter KI-Tools und klare Verbote für öffentliche Tools?                        | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 4  | Sind Training, Human Review, Datenhaltung, Löschung und Subprozessoren der Tools geprüft?             | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 5  | Werden wesentliche KI-Nutzungen in einem KI-Register dokumentiert?                                    | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 6  | Ist Human Review verbindlich, bevor KI-Outputs extern oder entscheidungsrelevant verwendet werden?    | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 7  | Gibt es Regeln für KI in Board-Sitzungen, Transkription, Protokollierung und Übersetzung?             | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 8  | Sind AI Avatare, synthetische Stimmen und KI-generierte Kommunikation gekennzeichnet und freigegeben? | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 9  | Sind agentische Workflows mit Freigabeschwellen, Logging und Kill-Switch geregelt?                    | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 10 | Gibt es einen Incident-Prozess für Fehloutput, Datenabfluss, Bias oder falsche Tool-Nutzung?          | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 11 | Sind Mitarbeitende, Freelancer und externe Beratende geschult und vertraglich eingebunden?            | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |
| 12 | Erhält das Board mindestens jährlich ein KI-Lagebild mit Chancen, Risiken und Massnahmen?             | <input type="checkbox"/> Ja <input type="checkbox"/> Teilweise <input type="checkbox"/> Nein |

## Anhang A: Schlankes KI-Register

| Use Case           | Tool   | Owner  | Datenzone | Nutzen                  | Risiko           | Kontrolle           | Status    |
|--------------------|--------|--------|-----------|-------------------------|------------------|---------------------|-----------|
| Board-Briefing     | [Tool] | [Name] | Gelb/Rot  | schnellere Vorbereitung | falsche Quellen  | Quellenprüfung      | Pilot     |
| Protokoll-Entwurf  | [Tool] | [Name] | Rot       | Zeitgewinn              | Vertraulichkeit  | Freigabe + Löschung | zu prüfen |
| AI Avatar Training | [Tool] | [Name] | Gelb      | Skalierung Schulung     | Täuschung/Rechte | Kennzeichnung       | Pilot     |

## Anhang B: 30-60-90-Tage-Plan

| Frist   | Fokus                | Ergebnis                                                                                    |
|---------|----------------------|---------------------------------------------------------------------------------------------|
| 30 Tage | KI-Lagebild          | Tools, Schatten-KI, Datenzonen, Quick Wins und Sofortregeln erfassen.                       |
| 60 Tage | Freigabe & Schulung  | Tool-Check, Verantwortlichkeiten, Pilot-Use-Cases, Schulung und KI-Register aufsetzen.      |
| 90 Tage | Governance verankern | Reporting, Review-Rhythmus, Incident-Prozess und Board-Kontrollfragen institutionalisieren. |

## Anhang C: Tool-Freigabe

|                  |                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Prüfpunkte       | Datenhaltung, Training, Human Review, Subprozessoren, Vertrag, Rollenrechte, Logging, Löschung, Exit, Support und Kostenfolge.   |
| Freigabeschwelle | Je vertraulicher die Daten und je externer die Wirkung, desto höher die Kontrolle: von Team-Freigabe bis Board-/Legal-Entscheid. |

# Rechtliche Anker und Quellen

Diese Musterweisung ersetzt keine unternehmens-, branchen- oder fallbezogene juristische Prüfung.  
Sie basiert auf öffentlich zugänglichen Leitlinien und Rechtsankern.

SAV-Wegleitung für den Umgang mit künstlicher Intelligenz: [https://www.sav-fsa.ch/documents/672183/2025869/SAV\\_KI%2BGuidelines%2B2024.pdf/68d5eab4-c2ad-50bd-506f-7ba6af15a839?t=1726488889628](https://www.sav-fsa.ch/documents/672183/2025869/SAV_KI%2BGuidelines%2B2024.pdf/68d5eab4-c2ad-50bd-506f-7ba6af15a839?t=1726488889628)

EDÖB: KI und Datenschutz: <https://www.edoeb.admin.ch/de/ki-und-datenschutz>

Fedlex: Bundesgesetz über den Datenschutz (DSG): <https://www.fedlex.admin.ch/eli/cc/2022/491/de>

Fedlex: Art. 321 StGB Berufsgeheimnis: [https://www.fedlex.admin.ch/eli/cc/54/757\\_781\\_799/de#art\\_321](https://www.fedlex.admin.ch/eli/cc/54/757_781_799/de#art_321)

EUR-Lex: Regulation (EU) 2024/1689, Artificial Intelligence Act: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

---

Sallenbach AG | AI & Innovation Consulting | [www.sallenbach.org](http://www.sallenbach.org) | [vero@sallenbach.org](mailto:vero@sallenbach.org)