THE AI-READY BOARD

by
Rene Schmidli

Rene Schmidli



Rene Schmidli, ein Finanzexperte mit über 30 Jahren Investmenterfahrung, deckte bereits 1993 als Finanzanalyst den Technologiesektor ab und begleitete im Jahre 2000 ein Tech-IPO in der Schweiz. Heute arbeitet er selbstständig in verschiedenen Verwaltungsrats- und Beratungsfunktionen. Im Dezember 2024 schrieb er, motiviert von der rasanten Entwicklung bei AI, seine CAS-Arbeit über Generative AI bei Mateusz Dolata an der Universität Zürich, um eine praxisnahe Betrachtung von AI-Strategie- und Governance-Themen in Verwaltungsräten vorzunehmen.

AI-Autonomie. Erst was sie darf. Dann was sie kann.

Dr. Frank Desiere



Dr. Frank Desiere ist CEO von CorTec in Freiburg i. Br. Das MedTech-Unternehmen entwickelt mit Brain Interchange ein implantierbares Brain-Computer-Interface, das 2025 erstmals beim Menschen implantiert wurde. Zuvor war er in Führungsfunktionen bei Roche und Nestlé tätig. Er ist Non-Executive Director und Faculty-Mitglied im Deloitte Board Programme. In seinem Newsletter und Podcast WE TALK BOARD schreibt er über Governance aus Schweizer und europäischer Sicht. Promotion an der ETH Zürich, MBA am IMD.

Was ein Hirnimplantat Verwaltungsräte über AI Agenten lehrt

Rene Schmidli: Frank, Du bist CEO von CorTec, einer MedTech-Firma, welche bidirektionale Gehirn-Computer Interfaces (BCI) entwickelt. Was kann ein Verwaltungsrat einer Bank oder eines Industrieunternehmens ausgerechnet von der Governance eines Hirnimplantats über AI-Agenten lernen?

Frank Desiere: Weil die Medizintechnik dieselbe Governancefrage in einer besonders harten Form kennt: Was passiert, wenn Technik nicht nur analysiert, sondern unmittelbar auf einen Menschen einwirkt? Bei einem implantierbaren Neurostimulationssystem können Folgen unmittelbar und sicherheitskritisch sein. Deshalb müssen Zweck, Grenzen, Risiken und Kontrollen vorab sehr präzise definiert und nachgewiesen werden.

Wenn ein AI Agent Rechnungen freigibt, Preise setzt oder Kundenanfragen abschliessend beantwortet, delegiert ein Unternehmen ebenfalls Handlung. Die Wirkung ist häufig verteilter und weniger sichtbar als bei einem Implantat, aber die Governancefrage ist dieselbe: Wer darf was entscheiden, innerhalb welcher Grenzen, und wer greift ein, wenn etwas schiefläuft? Deshalb ist MedTech für mich kein 1:1-Vergleich, sondern ein sehr illustratives Lernfeld für delegierte Handlung. Ein Beispiel aus CorTec: Zwischen unserer Gründung 2010 und der ersten Implantation von Brain Interchange beim Menschen im Juli 2025 in Seattle lagen 15 Jahre. Den Zeitpunkt bestimmte der Nachweis. Erst nach abgeschlossener Verifikation, Validierung und Risikoanalyse war der Schritt zum Patienten verantwortbar.

Rene Schmidli: Was heisst «delegierte Handlung» bei CorTec ganz konkret?

Frank Desiere: Brain Interchange ist ein vollständig implantierbares, drahtloses und bidirektionales Brain-Computer-Interface. Es zeichnet neuronale Signale auf und kann über dieselben Schnittstellen gezielt elektrisch stimulieren. Die Software verarbeitet die Daten und steuert das Implantat; für den geschlossenen Regelkreis spezifizieren wir eine Latenz von höchstens 25 Millisekunden. Je nach Anwendung können Erfassen, Verarbeitung und Stimulation damit zu einem Closed Loop verbunden werden. Entscheidend ist: «Closed Loop» bedeutet nicht freie Autonomie. Das System arbeitet innerhalb eines klinisch und technisch definierten Rahmens.

In der laufenden klinischen Studie entscheidet das System nicht frei. Die Ärztinnen und Ärzte des Studienteams legen die Stimulationsparameter fest, innerhalb der Grenzen, die Studienprotokoll und Systemdesign vorgeben. Sicherheitsrelevante Grenzen sind im System selbst verankert und lassen sich nicht per Einstellung überschreiten. Jede Änderung an diesen Grenzen durchläuft unseren Change-Prozess und, wo nötig, die Genehmigung durch Behörde und Ethikkommission.

Genau diese Kette bauen Unternehmen heute mit Agenten nach: Daten erfassen, interpretieren, entscheiden und ausführen. Der Unterschied ist weniger die Logik als die Disziplin darum herum. In regulierter MedTech müssen Risikomanagement, Designentscheidungen, Verifikation, Validierung und relevante Änderungen dokumentiert und nachvollziehbar sein. Bei Unternehmensagenten wird dieselbe Handlungskette oft viel schneller zusammengesetzt und die Governance hinkt oft entsprechend hinterher.

Rene Schmidli: Erkennen, empfehlen, entscheiden, selbständig ausführen: Ab welcher Stufe darf der Mensch aus der operativen Schleife heraus?

Frank Desiere: Ich würde die Grenze nicht aus der technischen Machbarkeit ableiten, sondern aus Zweck, Risiko, Reversibilität und den validierten Betriebsgrenzen. Für einen Unternehmensagenten wären für mich vor autonomer Ausführung mindestens drei Dinge nötig:

- erstens klar definierte und getestete Grenzen;
- zweitens eine real wirksame Möglichkeit für Menschen, einzugreifen oder zu übersteuern;
- drittens ein definierter Fallback, wenn das System unsicher ist oder ausserhalb seiner Grenzen gerät.

Ich möchte aber vor einer bequemen Antwort warnen: «Human in the Loop» ist kein Wert an sich. Wenn ein Sachbearbeiter täglich Hunderte Systemvorschläge nur noch bestätigt, ist er möglicherweise kein wirksamer Kontrolleur mehr, sondern ein Stempel. Der EU AI Act verlangt bei Hochrisiko-Systemen ausdrücklich wirksame menschliche Aufsicht und nennt dabei auch die Gefahr des «Automation Bias», also des blinden oder übermässigen Vertrauens in Systemoutputs.

Die Frage für den Verwaltungsrat lautet deshalb nicht: «Ist ein Mensch dabei?», sondern: Kann dieser Mensch realistisch eingreifen? Hat er die Information, die Zeit, die Kompetenz und die Autorität dazu? Wenn nicht, ist die menschliche Kontrolle nur formal und das System faktisch autonomer, als es im Organigramm aussieht.

Rene Schmidli: Wenn du aus der Medizintechnik nur zwei Disziplinen in die Unternehmenswelt übertragen könntest: Welche wären es?

Frank Desiere: Zuerst der Verwendungszweck. Viele Agenten werden nach dem Motto eingeführt: «Schauen wir, was geht.» Dabei macht ein einziger Satz einen grossen Unterschied. Ein Kundenservice-Agent, der «Auskunft zum Lieferstatus gibt», ist etwas anderes als einer, der «Kundenanliegen löst». Der zweite kann irgendwann Kulanz gewähren, Kündigungen entgegennehmen oder Zusagen machen. Genau deshalb muss vor dem Einsatz klar sein, wofür ein Agent da ist und wofür ausdrücklich nicht.

Zweitens der Funktionsnachweis. Ein gelungener Pilot oder eine eindrückliche Demo ist noch kein Nachweis, dass ein System unter definierten Bedingungen zuverlässig funktioniert. In MedTech muss die Leistung verifiziert und validiert werden, einschliesslich relevanter Grenz- und Nutzungssituationen. Im Unternehmenskontext besteht die Gefahr, dass ein Gremium vor allem die Demo sieht und zu wenig über Fehlerraten, Ausnahmefälle und Grenzen erfährt.

Im BCI-Feld erlebe ich das laufend. Videos von Patienten, die einen Cursor steuern, erzeugen Aufmerksamkeit. Investoren und Regulatoren fragen danach etwas anderes: Wie stabil ist das Signal über Monate? Wie oft versagt das System? Was passiert im Grenzfall? Diese Antworten entscheiden über Finanzierung und Zulassung. Dieselben Fragen gehören in jede Verwaltungsratssitzung, in der ein AI Agent zur Freigabe steht.

Rene Schmidli: Wer trägt die Verantwortung für einen Entscheid, den ein Agent autonom vorbereitet und ausführt?

Frank Desiere: Die erste Antwort ist einfach: Eine Maschine kann keine Organverantwortung übernehmen. Interessanter ist, was daraus für den Verwaltungsrat folgt. Art. 754 Abs. 2 OR sieht bei einer befugten Delegation an ein anderes Organ eine Haftungsentlastung vor, wenn bei Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt nachgewiesen wird.

Ein AI Agent ist aber kein «anderes Organ» im Sinn dieser Bestimmung. Deshalb würde ich nicht davon ausgehen, dass der Einsatz eines Agenten dieselbe haftungsrechtliche Entlastung auslöst wie eine ordnungsgemässe Delegation innerhalb der Organisation. Juristisch ist der Agent zunächst ein eingesetztes System oder Werkzeug; die menschliche Organisations-, Auswahl-, Instruktions- und Überwachungsverantwortung verschwindet dadurch nicht.

Praktisch heisst das für mich: Jeder Agent mit relevanter Ausführungskompetenz braucht einen namentlich bezeichneten Owner in der Linie, nicht bloss ein Projektteam oder die IT. In MedTech sind Hersteller- und Betreiberrollen regulatorisch klar adressiert. Im Unternehmen verteilen sich technische und fachliche Verantwortung schnell auf Anbieter, IT, Risk und Business; genau deshalb muss die interne Verantwortlichkeit explizit gemacht werden.

Meine Position ist klar: Wer AI einsetzt, bleibt für Auswahl, Instruktion und Überwachung des Systems verantwortlich. Verletzt der Verwaltungsrat diese Sorgfaltspflicht, haftet er nach Art. 754 OR persönlich. Eine D&O-Versicherung ersetzt diese Pflicht nicht, sie setzt sie voraus. Spezifische Rechtsprechung zu AI-Agenten kenne ich bisher nicht. Bis es sie gibt, plane ich als Verwaltungsrat konservativ.

Rene Schmidli: Wo bricht die Analogie zur Medizintechnik?

Frank Desiere: An drei Stellen. Erstens wird ein Medizinprodukt nicht einfach «eingefroren», aber seine freigegebene Konfiguration und jede relevante Änderung unterliegen einem kontrollierten Change-Prozess; je nach Änderung kann eine neue regulatorische Einreichung nötig werden. Ein Unternehmensagent kann dagegen auf einem externen Modell beruhen, dessen Verhalten sich durch Anbieter-Updates verändert, sofern Versionen und Änderungen nicht aktiv kontrolliert werden. Zweitens hat ein Medizinprodukt typischerweise einen eng definierten Zweck, während ein General-Purpose-Sprachmodell sehr breit einsetzbar ist. Drittens gibt es für viele interne Unternehmensagenten keine Behörde, die jeden einzelnen Use Case vorab genehmigt.

Die Konsequenz ist: Das Unternehmen muss einen Teil dieser Disziplin selbst organisieren. Besonders interessant ist der Ansatz der FDA für AI-enabled Device Software Functions: Ein «Predetermined Change Control Plan» kann bereits in der regulatorischen Einreichung festlegen, welche Modelländerungen geplant sind, wie sie entwickelt und validiert werden und wie ihre Auswirkungen beurteilt werden. Für Brain Interchange steht der PCCP heute nicht im Vordergrund, weil das System keine lernende AI-Komponente enthält. Entscheidend sind bei uns die Design-Change-Kontrolle im Qualitätsmanagementsystem nach ISO 13485 und die Abstimmung relevanter Änderungen mit Behörde und Ethikkommission.

Genau diese Logik würde ich für Unternehmensagenten übernehmen: Vorab festlegen, welche Änderungen eine neue Prüfung oder Freigabe auslösen, etwa ein neues Basismodell, zusätzliche Werkzeuge, erweiterte Systemberechtigungen, neue Datenzugriffe oder ein veränderter Verwendungszweck.

Rene Schmidli: Welche Entscheide würdest du, unabhängig davon, wie gut ein Agent technisch ist, aus Verwaltungsratssicht, nicht vollständig delegieren?

Frank Desiere: Sicher die unübertragbaren und unentziehbaren Aufgaben des Verwaltungsrats nach Art. 716a OR, etwa Oberleitung, Organisation, Finanzkontrolle und Oberaufsicht. Ein Agent kann Analysen, Varianten oder Beschlussentwürfe vorbereiten; die Wahrnehmung dieser Aufgaben bleibt beim Verwaltungsrat.

Weiter wäre ich bei Entscheidungen mit gravierenden Auswirkungen auf einzelne Menschen sehr zurückhaltend etwa bei Kündigungen, Kreditwürdigkeitsentscheiden oder medizinischen Behandlungsentscheidungen. Der EU AI Act stuft bestimmte Systeme im Personalbereich, einschliesslich Entscheidungen über Beendigung von Arbeitsverhältnissen, sowie Systeme zur Bewertung der Kreditwürdigkeit natürlicher Personen als Hochrisiko ein. Das ist kein generelles Verbot autonomer Entscheidungen, aber ein klares Signal für erhöhte Anforderungen an Governance und menschliche Aufsicht.

Auch gehört alles ausserhalb des definierten Verwendungszwecks zurück zum Menschen, ebenso wie echte Ziel- und Wertekonflikte, bei denen nicht nur optimiert, sondern abgewogen werden muss.

Zu guter Letzt: Entscheidungen über den Agenten selbst. Ein Agent sollte seine eigenen Berechtigungen nicht eigenmächtig erweitern, seine Limiten nicht selbst hochsetzen und seine Überwachung nicht abschalten können. Das ist keine philosophische Frage, sondern ein technisches Designprinzip: Rechte, Limits und Kontrollmechanismen müssen ausserhalb der Verfügung des Systems liegen, das sie begrenzen sollen.

Eine Kategorie würde ich zwingend ergänzen: irreversible Handlungen. Zahlungen, Vertragsabschlüsse und Erklärungen im Namen des Unternehmens lassen sich nicht einfach zurückholen. Hier braucht es ein Vier-Augen-Prinzip und die technische Möglichkeit, eine Zahlung oder Freigabe zu stoppen. Deepfake-Betrug mit der Stimme des CEO zeigt, warum: Ein ungutes Gefühl schützt niemanden. Schutz entsteht durch einen verbindlichen Prozess.

Rene Schmidli: Ab welchem Autonomiegrad muss ein AI-Use-Case dem Verwaltungsrat vorgelegt werden?

Frank Desiere: Der Verwaltungsrat sollte nicht jeden Agenten einzeln genehmigen; sonst wird er zum operativen Engpass. Seine Aufgabe ist der Rahmen: Risikoappetit, Autonomiestufen, klare Genehmigungskompetenzen, Vorlagekriterien sowie Reporting und Eskalation. Das Organisationsreglement regelt heute, welche Kompetenzen bei Verwaltungsrat und Geschäftsleitung liegen. Dieselbe Logik sollte künftig auch festlegen, unter welchen Bedingungen Maschinen selbständig handeln dürfen.

Vorlagepflichtig würde ich einen Use Case machen, wenn zwei Dinge zusammenkommen: Der Agent entscheidet oder führt selbständig aus, und die Wirkung trifft Kunden, Mitarbeitende, Finanzen, Compliance oder Reputation wesentlich.

Eine Ausnahme würde ich bewusst machen: Die ersten Agenten mit eigener Ausführungskompetenz sollte ein Verwaltungsrat selbst sehen und erleben, nicht um Mikromanagement zu betreiben, sondern um ein realistisches Bild davon zu bekommen, wie sich solche Systeme unter realen Bedingungen verhalten.

Ebenso wichtig ist, worüber der Verwaltungsrat informiert wird. Umfragen wie der swissVR Monitor zeigen, dass ein erheblicher Teil der Verwaltungsräte nicht regelmässig über Einsatz und Risiken von AI informiert wird. Ohne dieses Reporting kann ein Verwaltungsrat seine Oberaufsicht nach Art. 716a OR nicht wahrnehmen.

Rene Schmidli: Braucht es Kompetenz-, Betrags- oder Risikolimiten für AI-Agenten?

Frank Desiere: Ja, faktisch ein Funktionendiagramm für Agenten. Jeder Verwaltungsrat kennt das Prinzip: Wir regeln, wer was entscheiden oder bis zu welchem Betrag freigeben darf. Warum sollte ein Agent, der Bestellungen auslöst oder Zahlungen vorbereitet, ohne vergleichbare Kompetenzgrenzen arbeiten?

Die Limiten sollten mehrere Dimensionen abdecken: Betrag, Art der Handlung, Systemzugänge, Gegenparteien, Frequenz, Datenzugriff und Eskalationsschwelle. Ein Einkaufsagent könnte zum Beispiel bei bestehenden Lieferanten bis CHF 5'000 bestellen, aber keine neuen Lieferanten anlegen und höchstens eine definierte Zahl von Bestellungen pro Tag auslösen. Alles darüber geht an einen Menschen.

Und ich würde Agenten behandeln wie neue Mitarbeitende in der Probezeit: niedrige Kompetenzen am Anfang, Ausweitung erst nach nachgewiesener Zuverlässigkeit. In MedTech würde man eher von validierten Betriebs- und Leistungsgrenzen sprechen. Für Unternehmen ist es im Kern dasselbe Führungsprinzip: Vertrauen wird nicht angenommen, sondern anhand von Evidenz erweitert.

Rene Schmidli: Wie muss sich das interne Kontrollsystem verändern, wenn nicht nur Menschen, sondern auch Agenten Transaktionen ausführen?

Frank Desiere: Viele klassische IKS-Kontrollen sind um menschliche Rollen, Freigaben, Funktionentrennung und Stichproben herum gebaut. Wenn ein Agent sehr viele Transaktionen in kurzer Zeit ausführen kann, reichen rein periodische oder stichprobenbasierte Kontrollen allein nicht mehr aus. Ein Teil der Kontrolle muss deshalb näher an die einzelne Transaktion und an die Systemlogik rücken.

Das schärfste Beispiel ist die Funktionentrennung. Wenn derselbe Agent einen neuen Lieferanten anlegen und anschliessend eine Zahlung an diesen Lieferanten auslösen kann, ist eine zentrale Kontrollidee ausgehebelt. Das Risiko entsteht besonders dann, wenn Agenten aus Bequemlichkeit mit sehr breiten Berechtigungen ausgestattet werden. Deshalb braucht auch ein Agent Least-Privilege und sauber getrennte Rollen.

Kontrollen müssen deshalb teilweise in das System wandern: technische Leitplanken, lückenlose Protokollierung relevanter Handlungen, eigene Identitäten und Berechtigungen für Agenten, Schwellenwerte und ein Vier-Augen-Prinzip dort, wo das Risiko es verlangt. Dazu braucht auch die zweite Verteidigungslinie genügend AI-Kompetenz.

Ein Punkt wird oft übersehen: Agenten werden selbst zum Angriffsziel. Mit ihren Zugriffsrechten, ihrem Gedächtnis und ihren Werkzeugen sind sie für Angreifer attraktiv, etwa über Prompt Injection. Anthropic hat im November 2025 eine Spionagekampagne offengelegt, bei der AI rund 80 bis 90 Prozent der Operation selbständig ausführte. Deshalb gehören Agenten in ein Zero-Trust-Konzept mit eigenen Identitäten und eng begrenzten Berechtigungen.

Und der Verwaltungsrat sollte die Revisionsstelle fragen, wie agentengetriebene Prozesse in der IKS-Prüfung berücksichtigt werden. Bei der ordentlichen Revision prüft die Revisionsstelle nach Art. 728a OR, ob ein IKS existiert; daraus folgt nicht automatisch eine umfassende Wirksamkeitsprüfung jedes AI-Kontrollmechanismus.

Rene Schmidli: Reicht periodisches Reporting noch aus, oder braucht es für Agenten kontinuierliche Überwachung?

Frank Desiere: Beides, aber auf unterschiedlichen Ebenen. Operativ braucht es kontinuierliche Überwachung. In der Medizintechnik endet die Kontrolle nicht mit Zulassung oder Inverkehrbringen: Die EU Medical Device Regulation (MDR) verlangt ein Post-Market-Surveillance-System, das über den gesamten Lebenszyklus relevante Daten zu Qualität, Leistung und Sicherheit aktiv und systematisch sammelt und auswertet. Der übertragbare Gedanke ist: Go-live ist der Beginn der Überwachung, nicht ihr Ende.

Der Verwaltungsrat braucht deshalb kein Echtzeit-Dashboard für jeden Agenten, aber ein Reporting, das Reifegrad und Risiko zeigt statt bloss Aktivität. Mich interessiert nicht primär, wie viele Agenten im Einsatz sind, sondern: Auf welcher Autonomiestufe arbeiten sie? Welche Limiten gelten und wie stark werden sie

genutzt? Wie oft greifen Menschen ein? Welche Vorfälle und Ausnahmen gab es? Und hat sich das Verhalten nach einem Modell- oder Tool-Update messbar verändert?

Dazu kommen zwei Dinge, die kein Reporting ersetzt: eine klare Ad-hoc-Eskalation bei schweren Vorfällen und die Fähigkeit, einen Agenten kontrolliert zu stoppen oder auf einen sicheren manuellen Prozess zurückzufallen. Die entscheidende Prüffrage lautet: Läuft der kritische Prozess morgen weiter, wenn der Agent ausfällt? Der EU AI Act verlangt für Hochrisiko-Systeme, dass menschliche Aufsicht bei Bedarf eingreifen oder das System in einen sicheren Halt bringen kann. In MedTech ist das verwandte Prinzip ein risikokontrollierter Fallback, nicht zwingend überall derselbe Begriff «sicherer Zustand».

Rene Schmidli: Du bist CEO von CorTec und zugleich als Non-Executive Director tätig. Wo spürst du bei Agentic AI die Spannung zwischen operativer Führungsverantwortung und Aufsicht am stärksten?

Frank Desiere: Als CEO will ich Tempo: Ich sehe Effizienz, Wettbewerb und den Druck, neue Möglichkeiten früh zu nutzen. Als Non-Executive Director stelle ich eine andere Frage: Sind Zweck, Grenzen, Verantwortung und Evidenz so klar, dass ich diese Delegation mittragen kann? Diese Spannung sollte man nicht auflösen. Sie ist produktiv, solange Rollen und Entscheidungsrechte sauber getrennt bleiben.

Was ich aus MedTech mitnehme: Klare Leitplanken sind kein Gegenstück zu Tempo; sie sind die Voraussetzung, Tempo zu skalieren. Wenn Autonomiestufe, Limiten, Monitoring und Fallback vorab definiert sind, muss das Unternehmen nicht jeden Einzelfall neu verhandeln. Wer diese Grundlagen nicht hat, wird entweder unnötig vorsichtig oder erst durch einen Vorfall gezwungen, die Grenzen nachträglich zu definieren.

Mein Grundsatz gilt in beiden Rollen: Unsere Aufgabe ist es, konsequent die richtigen Fragen zu stellen. Bauen und betreiben muss das Management. Und AI gehört in das bestehende Risiko- und Resilienzmanagement des Unternehmens, nicht in die IT-Ecke.

Rene Schmidli: Ein Satz an einen Verwaltungsratspräsidenten, der nächste Woche den ersten Agenten mit eigener Ausführungskompetenz freigeben soll?

Frank Desiere: Delegieren Sie an eine Maschine mit derselben Sorgfalt wie an einen Menschen. Entscheiden Sie zuerst, was das System darf. Erst danach zählt, was es kann.