

# THE AI-READY BOARD

by  
Rene Schmidli

Rene Schmidli



René Schmidli, ein Finanzexperte mit über 30 Jahren Investmentenerfahrung, 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.

David Rosenthal



David Rosenthal ist seit 30 Jahren im Bereich Daten- und Technologierecht tätig, hat sowohl ein Jurastudium an der Universität Basel als auch einen Background als Software-Engineer und ist Partner der Wirtschaftskanzlei VISCHER, wo er unter anderem das Data & AI-Team und jenes für interne Untersuchungen leitet. Er ist bekannt für seine Methoden zur Risikobeurteilung beim Einsatz von Cloud- und AI-Techniken, seine Publikationen (und speziell den AI-Blog [vischer.com/ki](https://vischer.com/ki)) sowie sein KI-Tool «Red Ink» ([redink.ai](https://redink.ai)). Er ist zudem Dozent an der Universität Basel und der ETH Zürich.

**«Sovereign AI:  
Wunsch und  
Realität auf dem  
Prüfstand»**

---

***Trotz US-Dominanz bei der Infrastruktur und dem US-CLOUD-Act: Dank hybriden Lösungen und einem risikobasierten Ansatz verpasst keiner den Anschluss***

---

**René Schmidli:** Lieber David. Beginnen wir mit den Grundlagen. Was verstehst du unter «Sovereign AI» aus Sicht einer Schweizer Unternehmung?

**David Rosenthal:** Für mich ist das zunächst ein Schlagwort, das sich in aller Munde befindet und das den menschlichen Urwunsch zum Ausdruck bringt, nicht von Fremden abhängig zu sein – in diesem Fall in Sachen künstliche Intelligenz. Das ist derzeit deshalb ein grosses Thema, weil wir spüren oder sogar realisieren, dass AI für uns in Zukunft enorm wichtig sein wird, wir aber gleichzeitig das Gefühl haben, nicht wirklich Kontrolle über diese Ressource zu haben. Weil der Aufbau von AI sehr kostenintensiv ist, befürchten wir wohl zu Recht, dass sehr leistungsfähige AI künftig nur aus den Händen weniger verfügbar sein wird. Das sind alles Gefühle, geprägt von einzelnen Erfahrungen, Eindrücken und Umständen, aber das macht sie nicht weniger relevant. Darum ist das Thema in der Politik derzeit hoch im Kurs. In der Privatwirtschaft ist es umgekehrt viel weniger ein Thema, weil hier Pragmatismus, Opportunismus und Sachlichkeit dominieren, auch wenn hier natürlich auch niemand gern abhängig ist. Thematisch ist das Streben nach «digitaler Souveränität» derzeit vor allem eine Gegenbewegung zum Umstand, dass die meiste der wirklich leistungsfähigen AI von grossen US-Tech-Konzernen kommt und viele meinen, das Rezept zur Schaffung von «souveräner AI» bestehe darin, in Europa ebensolche AI aufzubauen. Das ist angesichts der politischen Weltlage natürlich naheliegend, aber letztlich würde dadurch nüchtern betrachtet erstens eine Abhängigkeit durch eine andere ersetzt, und zweitens ist es unwahrscheinlich, dass ein europäisches Produkt den grossen AI-Modellen aus den USA und China je wirklich das Wasser reichen können wird. Die Fronten sind in dieser

Diskussion allerdings leider verhärtet und es wird auch kaum sachlich diskutiert. Das führt zu einer erheblichen Verunsicherung der Entscheidungsträger und im öffentlichen Sektor zu einer Stagnation im Bereich der Digitalisierung, was niemandem dient. Das ist schade.

**René Schmidli:** Dabei sind Abhängigkeiten im IT-Bereich nichts Neues ...

**David Rosenthal:** Genau. Ich berichtete darüber schon vor über 30 Jahren, als ich noch als Tech-Journalist unterwegs war. Schon damals wählte die Masse das, was für sie am bequemsten war, und nicht, was die geringsten Risiken mit sich brachte oder am besten war. Das ist heute nicht anders. Technologie wird nach wie vor weder moralisch noch politisch gekauft, sondern opportunistisch. Weil das aber mit einem guten Gewissen geschehen soll, wird wie üblich mit Schlagwörtern operiert, und «Sovereign» ist eins davon. So ist es derzeit in Mode, dass grosse US-Tech-Anbieter in Europa Angebote lancieren, bei welchen die US-Mutterkonzerne keinerlei technischen Zugriff auf die Daten haben sollen. Aber wären wir damit wirklich unabhängig? Woher kommen die Software-Updates, ohne die unsere Lösungen nicht überleben können? Kann Europa das Internet unabhängig von den USA betreiben? Woher kommen die Chips, die es für den Betrieb von AI in grossen Mengen braucht? Woher kommen die Modelle? Und selbst wenn wir die Software selbst schreiben: Woher kommen die Werkzeuge und Bibliotheken, mit denen wir das machen? Zu einem grossen Teil nicht aus Europa und sicher nicht aus der Schweiz. Und wenn Unternehmen dann für einen abgeschoteteten Server in Europa mehr bezahlen sollen, weniger rasch Updates und nur die vorletzte Generation der AI-Modelle erhalten, werden sie sich trotzdem dafür entscheiden? Die Erfahrung sagt nein. Sie werden stattdessen eine pragmatisch-realistische Risikobeurteilung vornehmen und mindestens versuchen, nicht alles auf eine Karte zu setzen und sich so ihre «digitale Souveränität» wenigstens ein ganz wenig zu bewahren. Das ist aber in der Praxis weniger eine Angelegenheit USA vs. Europa, sondern Diversifikation, wo es eben gerade passt – bei Technologie, bei Anbietern und bei Lösungsansätzen. Das gilt aber nur für jene, die sich das leisten können.

**René Schmidli:** Will heissen?

**David Rosenthal:** Dass Diversifikation nicht zum Nulltarif kommt und gerechtfertigt werden muss. Welches Unternehmen kann sich das Know-how leisten, beispielsweise seine Geschäftsanwendungen verteilt auf den Plattformen von zwei Hyperscalern gleichzeitig aufzubauen oder hybride Lösungen zu betreiben, so dass nicht nur Konkurrenz erhalten bleibt, sondern auch eine Alternative besteht, wenn alle Stricke reissen? Die Schweiz ist eine Microsoft-Hochburg. Es ist bequem, die Lösungen von Microsoft einzusetzen, auch wenn gewisse Produkte von Microsoft wie etwa Copilot für M365 meiner Meinung nach eine reine Enttäuschung sind. Wir sind bei uns (VISCHER) bewusst nicht diesen Weg gegangen und haben zu den Office-Produkten von Microsoft im Bereich AI etwas Eigenes entwickelt, das nach unserer Ansicht viel besser ist als Copilot für M365, und die Benutzer geben uns auch Recht. Aber diesen Wettbewerbsvorteil zu erlangen, den wir heute gegenüber unseren Mitbewerbern damit haben, erforderte Mut und Energie. Wir nutzen für AI zum Beispiel nicht Microsoft, sondern Google, könnten aber jederzeit umstellen, wenn das nötig wäre, weil unsere Lösung mit beliebigen AI-Modellen funktioniert. Wir sind damit nicht nur unabhängiger, sondern können unseren Benutzern nach unserer Ansicht zu tieferen Kosten eine wesentlich bessere AI-Lösung für den Alltag bieten, als die gängigen AI-Tools der US-Tech-Anbieter es können.

**René Schmidli:** Du plädiert also für den Einsatz von Open-Source-Produkten anstelle der etablierten Lösungen?

**David Rosenthal:** Nein, ich gehöre nicht zur Fraktion derjenigen, die quelloffene Software als Patentrezept sehen, auch wenn diese derzeit besonders viel Gehör erhalten. Es braucht einen Mix und es braucht mehr nüchterne Risikobetrachtung. Für mich gibt es drei Dinge, auf die wir in Unternehmen achten müssen: Funktionalität, Informationssicherheit und Sicherung der Geschäftsfortführung, also Business Continuity, wie man so schön sagt. Der Preis für Technologie ist in etablierten Märkten heute insgesamt überall ähnlich; tiefere Kosten dürften auch noch nie ein Grund dafür sein, in die Cloud zu gehen. Ein guter Grund ist hingegen die Informationssicherheit: Hier können die drei Hyperscaler Microsoft, Google und AWS mehr bieten

als der Eigenbetrieb, wenn ich Experten unserer Klienten glauben darf. US-Tech ist aber nicht pauschal besser. Den grossen AI-Anbietern wie OpenAI, Anthropic oder Perplexity traue ich bezüglich Informationssicherheit beispielsweise noch nicht zu, in dieser Liga zu spielen. Sie müssen aus meiner Sicht zuerst «erwachsen» werden. Darum sollten in sensiblen Bereichen andere Anbieter genutzt werden. Auch Microsoft & Co. mussten über die letzten fünf bis zehn Jahre in dieser Hinsicht reifen, wie wir das in zahlreichen Cloud-Projekten unserer Klienten miterlebt haben und noch immer gibt es Verbesserungsbedarf. Wenn mir aber selbst die Security-Profis von Schweizer Unternehmen mit hoher eigener IT-Sicherheit sagen, dass sie den Cloud-Providern nicht das Wasser reichen können, gibt mir das zu denken. Wenn dann kantonale Datenschützer der Öffentlichkeit noch immer weismachen wollen, Daten der öffentlichen Hand seien grundsätzlich sicherer, wenn sie auf eigenen Servern betrieben werden, haben sie den Sinn für die Realität verloren und machen ihre Hausaufgaben nicht. Ich habe öffentliche Verwaltungen gesehen, da war mehr als die Hälfte der Server nicht auf dem neusten Stand und verletzte damit schon das kleine Einmaleins der Informationssicherheit. Da nützt es auch nichts, wenn darauf nur Open Source läuft. Auch Open-Source-Software muss von irgendwem betrieben und gewartet werden. Nur weil der Quellcode frei verfügbar ist, bedeutet das nicht, dass keine Abhängigkeiten bestehen und eine Lösung sicherer ist. Ich sage dies, obwohl ich quell-offene Software für eine ausgezeichnete Sache halte; auch unsere AI-Lösung ist quelloffen. Aber die Welt ist auch in diesem Bereich nicht schwarz-weiss. Es entbehrt allerdings nicht einer gewissen Ironie, dass die heute besten einigermassen offenen AI-Modelle wie DeepSeek, Qwen oder Kimi aus China kommen. Sie werden bei uns für den Bau von «souveränen» AI-Lösungen besonders gern eingesetzt. Chinas Streben nach «Sovereign AI» kommt also auch uns zugute und ist letztlich eine direkte Folge der Handelspolitik der USA. Der Markt funktioniert also noch, irgendwie.

**René Schmidli:** Du sprichst mit deinem Seitenhieb auf die Datenschützer auch die rechtliche Dimension an. Hier fällt oft der Begriff «CLOUD Act». Was hat es damit auf sich?

**David Rosenthal:** Das ist ein Gesetz im US-Recht, mit dem 2018 geklärt wurde, dass Gerichte in den USA US-Provider auch dann zur Herausgabe von Daten ihrer Kunden für ein Strafverfahren verpflichten können, wenn diese die Daten im Ausland lagern. Das entspricht der Regelung, die wir hier in Europa und auch in der Schweiz haben. Die fragliche Bestimmung geht auf Art. 18 der Cyber-Crime-Convention des Europarats zurück, ist also keine amerikanische Erfindung. Wenn ein Schweizer Provider von einer Schweizer Staatsanwaltschaft zur Herausgabe von Kundendaten verpflichtet wird, kann er sich nicht mit dem Argument wehren, dass der Server im Ausland steht, was logisch ist. Den CLOUD Act haben wir übrigens nur, weil die US-Muttergesellschaft von Microsoft sich dort trotzdem wehrte und völlig überraschend Recht bekam. Da wurde der Punkt klargestellt. Es hat also nichts damit zu tun, dass die US-Regierung auf Daten europäischer Kunden zugreifen will.

**René Schmidli:** Sind die Befürchtungen, dass sich US-Behörden ohne Vorabinformation an die Unternehmung beliebig an Daten von Schweizer Unternehmen bedienen, real?

**David Rosenthal:** Natürlich sind diese Befürchtungen real, aber sie sind bei Lichte betrachtet im geschäftlichen Kontext in aller Regel unbegründet. Es gibt hier viel Angstmache und Unwissenheit, was es mit dem CLOUD Act auf sich hat, speziell von Datenschutzbehörden. Ich habe ein Gutachten von einem hoch angesehenen Schweizer Professor gesehen, das grundlegende fachliche Fehler zum CLOUD Act enthält; ich habe diese in einer Publikation dargelegt. So wird regelmässig suggeriert, die US-Behörden hätten quasi freien Zugriff auf die Daten der europäischen Geschäftskunden. Das stimmt schlicht nicht. Schon technisch besteht beim richtigen Setup und Cloud-Provider aus den USA grundsätzlich kein Zugriff auf Datenebene. Bei Microsoft meine ich zum Beispiel die "European Data Boundary", die Speicherung von Daten in Schweizer Rechenzentren sowie Vorkehrungen wie die "Customer Lockbox" oder die Customer-Managed-Key-Verschlüsselung bei Azure.. Rechtlich sind die Hürden nach US-Recht hoch, weshalb es in den Konstellationen, die uns hier interessieren, nach Aussagen etwa eines hochrangigen Vertreters von Microsoft in einer offiziellen Anhörung noch zu keinen solchen Zugriffen kam; in der Öffentlichkeit wurde hingegen nur seine

Aussage diskutiert, dass er die Preisgabe von Daten nicht zu 100% ausschliessen könne. Schutz vor Zugriffen gibt es allerdings nicht zum Nulltarif; es müssen diverse Vorkehrungen wie die erwähnten getroffen werden. Das Ergebnis ist, dass die Wahrscheinlichkeit eines US-Behördenzugriffs zwar nicht ausgeschlossen werden kann, aber nach allgemeiner Auffassung höchst unwahrscheinlich wird. Das Problem ist, dass eine Gruppe radikaler Datenschützer behauptet, das Risiko müsse null sein und daher so tun, als sei die Cloud-Nutzung jedenfalls für die öffentliche Hand verboten, was natürlich nicht stimmt. Beim Schutz vor Hackern aus China und Russland legen sie notabene völlig andere Massstäbe an. Obwohl das alles nicht aufgeht und keinen Sinn macht, sorgt es für erhebliche Verunsicherung, was auch dem Datenschutz schadet. Auch die Privatwirtschaft wie etwa bei den Banken hat sich mit dem Thema beschäftigt und es aufgearbeitet. Hier genügt es, dass ein solcher Zugriff mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann, und das kann mit den richtigen Vorkehrungen auch bei Hyperscalern erfüllt werden, und zwar ganz ohne die realitätsfremden Forderungen so mancher Datenschützer (wie etwa die End-to-End-Verschlüsselung, die bei Diensten wie M365 keinen Sinn machen). Wir machen regelmässig entsprechende Workshops, in denen wir mit unseren Klienten die Risiken beurteilen, übrigens auch unter Berücksichtigung der Trump-Administration. Wir haben hierzu so weit ich das sehe als die einzigen im Markt eine Methodik zur Risikobeurteilung entwickelt.

**René Schmidli:** Du sprichst dein Risikomodell für sogenannte «Lawful Access»-Risiken an, das du vor Jahren entwickelt hast und das unter anderem der Kanton Zürich für seine Cloud-Entscheidung nutzt?

**David Rosenthal:** Ja, und auch die Finanzindustrie, Spitäler und viele andere, die dem Berufs- oder Amtsgeheimnis unterliegen. Es ist Open Source und mittlerweile der Standard für diese Beurteilungen. Ziel war es, die Diskussion zu versachlichen und die Problematik fassbar zu machen, indem das Problem sozusagen in kleinere Teile zerlegt wird. Diese werden dann in der Gruppe behandelt, was den Vorteil mit sich bringt, dass am Ende die diversen Stakeholder wie Legal, Datenschutz, Infosecurity, Business, IT etc. ein Verständnis für das Risiko haben und es vernünftig beurteilen können, zu welchem Ergebnis auch immer sie kommen. Der Sinn und Zweck solcher Risikobeurteilungen ist nicht einfach nur das Ermitteln einer Eintrittswahrscheinlichkeit, sondern das Bestreben, diese durch möglichst viele Massnahmen möglichst tief zu halten. Es geht darum, ein Thema systematisch anzugehen und nicht aus dem hohlen Bauch heraus zu entscheiden. Die Teilnehmer sind zum Beispiel regelmässig erstaunt, wenn wir ihnen anhand von Zahlen des Bundesamts für Justiz zeigen, dass es in über 95 Prozent der Fälle genügt, wenn die US-Strafverfolgungsbehörden den Schweizer Behörden ein Rechtshilfeersuchen stellen und so ganz normal an die Daten von Schweizer Behörden und Unternehmen herankommen. Da fällt die Notwendigkeit eines Zugriffs auf die Cloud schon von vornherein weg. Irgendwann wird sich diese Erkenntnis auch im öffentlichen Sektor durchsetzen. Der Bundesrat hat die USA übrigens auf die Liste der Staaten mit angemessenem Datenschutz gesetzt, trotz des CLOUD Acts.

**René Schmidli:** Ist die Cloud von US-Anbietern also überhaupt kein Problem?

**David Rosenthal:** Oh doch, da gibt es genügend Herausforderungen, aber sie liegen woanders. Wer seine Daten und digitalen Geschäftsprozesse einem Cloud-Provider anvertraut, macht sich von diesem abhängig womit wir wieder beim Thema sind. Fällt ein solcher aus oder gehen Daten verloren, steht der eigene Betrieb still. Da kann man noch so viel in die Verträge reinschreiben, weil dadurch der laufende Geschäftsbetrieb nur bedingt geschützt wird. Das heisst zwar nicht, dass Verträge unwichtig sind. Aber ein Unternehmen sollte, wenn es in die Cloud geht, einen Plan B und vielleicht auch einen Plan C haben, falls es diesen Provider rasch verlassen muss oder plötzlich nicht mehr auf seine Daten und Funktionen zugreifen kann. Ein Fokusbereich ist auch die Informationssicherheit; der Zugriff von ausländischen Behörden ist in unseren Cloud-Risiko-Beurteilungsmethoden nur einer von Dutzenden Prüfpunkten, die abgearbeitet werden müssen. Die Lösungen, die diese Anbieter uns bereitstellen, sind teilweise so mächtig, dass es eine Herausforderung für sich sein kann, sie wirklich im Griff zu haben und sicherzustellen, dass sie einem nicht um die Ohren fliegen. Das Problem ist also oft nicht, ob Google oder Microsoft die Sicherheit oder Business Continuity im Griff

haben, sondern ob das auch seitens der Kunden der Fall ist. Die Unternehmensleitung sollte sich zum Beispiel fragen: Haben wir ein Backup unserer Mails und Daten ausserhalb der Cloud und wären wir in der Lage, bei einem Ausfall innert nützlicher Frist auf ein alternatives System umzusteigen? Im AI-Bereich haben wir dieses Problem zum Glück weniger ausgeprägt, weil hier häufig «Zero Data Retention» praktiziert wird, also beim Provider nichts gespeichert wird. Dafür haben wir hier andere Herausforderungen, etwa die Überwachung durch Provider (Stichwort "Abuse Monitoring"). Oder dass Mitarbeitende auf privat eingesetzte AI-Angebote ausweichen, weil ihnen im Unternehmen nichts Vernünftiges angeboten wird. Das kann gefährlich werden.

**René Schmidli:** Warum?

**David Rosenthal:** Weil bei Angeboten für Konsumenten, wie wir sie typischerweise auf dem Handy haben, viele der Vorkehrungen gegen fremde Zugriffe nicht bestehen. Dasselbe gilt, wenn ich Leistungen direkt in den USA einkaufe, was bei grösseren etablierten Cloud-Providern nicht mehr der Fall ist. Bei diesen Consumer- oder US-Angeboten ist das Risiko eines Behördenzugriffs je nach Konstellation durchaus real. Wenn in der Presse davon berichtet wird, dass die Cloud-Provider einen Kunden den Behörden ausgeliefert haben, dann sind das in der Regel solche Fälle. Ein anderes Risiko ist der Einsatz von Providern, welche die Daten der Kunden möglicherweise noch für eigene Zwecke nutzen. Oder die nicht bereit sind, unseren Schutzstandard zu bieten. So gibt es bekannte Anbieter von AI-Services wie OpenAI, die wir zum Beispiel nie mit Berufsgeheimnisdaten nutzen würden. Das schränkt die Auswahl zwar etwas ein, aber es gibt Lösungen, im Cloud-Bereich etwa mit Google und je nach Setup mit Microsoft und natürlich bei Schweizer Anbietern.

**René Schmidli:** Viele Verwaltungsräte fragen sich: «Wenn wir weniger abhängig sein wollen, welche Alternativen haben wir?» Was sagst du zu europäischen und Schweizer Cloud- und AI-Lösungen?

**David Rosenthal:** An die drei US-Hyperscaler kommen die europäischen Anbieter im Kerngeschäft der Hyperscaler nach mehrheitlicher Auffassung leider nicht heran. Darum wird die Abhängigkeit von ihnen auf absehbare Zeit hoch bleiben. Immerhin gibt es drei davon. Ich rechne nicht mit einem europäischen Gegenangebot auf diesem Niveau. Das finde ich nicht gut, aber wir müssen realistisch bleiben. Daher gehe ich auch nicht davon aus, dass die Leute in Scharen M365 hinter sich lassen. Allerdings gibt es manche Bereiche, wo die Hyperscaler nicht dominieren, und da gibt es gute andere Lösungen, etwa was Geschäftsanwendungen betrifft. Darum kann ich zwei Dinge empfehlen: Erstens den erwähnten Plan B ausarbeiten und die eigene Geschäftsführung sichern, auch wenn der Plan B weniger attraktiv ist. Und zweitens, wie schon erwähnt, diversifizieren. Wir haben bei uns in der Kanzlei zwar ebenfalls M365, weil dies für uns die attraktivste Lösung ist. Aber wir haben unsere Dokumente und weitere Applikationen in einem Schweizer Rechenzentrum beim Schweizer Provider MTF. Im Bereich AI wollen wir die besten Modelle, weil wir AI intensiv einsetzen. Darum sind wir dort mit Google unterwegs. Weil Microsoft sich zierte, als es um die Absicherung unserer Daten ging, haben wir beim Konkurrenten angeklopft, und dort empfing man uns mit offenen Armen. Hier spielte der Wettbewerb also. Es gibt freilich gute Schweizer AI-Lösungen für all jene, die den Cloud-Anbietern nicht trauen oder ihre Angebote aus politischen Gründen nicht nutzen wollen oder dürfen. Es sind gewisse Leistungseinbussen zu akzeptieren, was je nach Anwendung aber kaum ins Gewicht fällt.

**René Schmidli:** Viele politische Debatten bzw. unternehmerisch getriebene Initiativen suggerieren, man könne die vollständige Unabhängigkeit erreichen, wenn man nur genug «Sovereign» baut. Ist das aus deiner Sicht realistisch und wäre es überhaupt wünschenswert?

**David Rosenthal:** Nein und nein. Vollständige Unabhängigkeit gibt es, wie erwähnt, nicht. Ich hätte sie nur dann, wenn jede in der gesamten digitalen Wertschöpfungskette eingesetzte Komponente nicht nur technisch frei austauschbar wäre, sondern auch von genügend vielen Anbietern bereitgestellt würde. So funktioniert der IT-Markt nicht, und es gäbe auch keine Innovation. Zudem baut die Effizienz unserer Wirtschaft darauf, dass wir sie arbeitsteilig organisieren und jene Dinge, die andere für uns besser machen können, von ihnen machen lassen, womit wir Abhängigkeiten schaffen. Darum ist vollständige Unabhängigkeit nicht

wünschenswert; wir müssten auf Effizienzen und andere Vorteile verzichten. Es ist jedoch wichtig, dass es Regulative gibt. Zum Beispiel den Wettbewerb, in dem neue Anbieter die bestehenden unter Druck setzen, sei es punkto Preis, Konditionen oder Innovation. Im Bereich der AI spielt dieser Wettbewerb im Moment noch. Das andere Regulativ ist das Recht, namentlich das Wettbewerbsrecht, das dann einschreitet, wenn eine marktmächtige Position in unerwünschter Weise ausgenutzt wird. Das geschieht auch immer wieder. So läuft gerade in der Schweiz eine Vorabklärung der Wettbewerbskommission gegen Microsoft betreffend deren Lizenzpreise für M365. Es ist allerdings kein agiles Instrument, und Microsoft ist mittlerweile «too big to fail» für die digitale Wirtschaft. Die meisten haben allerdings mehr Sorge, dass Trump Microsoft als Waffe gegen die Europäer einsetzt, als dass andere Umstände zum grossen Crash oder Breach bei Microsoft führen. Mir macht Letzteres mehr Sorge.

**René Schmidli:** Was also sind deine Empfehlungen für Schweizer Verwaltungsräte, insbesondere beim Einsatz von Cloud und AI?

**David Rosenthal:** Erstens: Lassen Sie sich nicht von Schlagworten wie «Sovereign AI» oder der emotionalen Diskussion rund um den CLOUD Act verunsichern. Treffen Sie Ihre Entscheide sachlich und risikobasiert, möglichst nicht aus dem Bauch heraus. Aber machen Sie Ihre Hausaufgaben. Der Cloud-Einsatz lässt sich unterschiedlich gestalten. Sorgen Sie nicht nur für die richtigen Verträge, sondern auch für die richtigen weiteren technischen und organisatorischen Massnahmen.

Zweitens: Akzeptieren Sie, dass es keine vollständige Unabhängigkeit gibt. Konzentrieren Sie sich stattdessen auf die Beherrschung der realen Risiken. Die grössten Gefahren sind aus meiner Sicht nicht ausländische Behörden, sondern Betriebsausfälle, Verletzungen der Informationssicherheit, mangelnde interne Kontrolle und fehlendes Know-how über die mächtigen Werkzeuge, die Sie einsetzen.

Drittens: Sorgen Sie für einen Plan B. Was tun Sie, wenn Ihr Hauptanbieter ausfällt? Können Sie Ihre Daten rasch migrieren? Diversifizieren Sie, wo es wirtschaftlich sinnvoll ist, um Abhängigkeiten zu reduzieren und den Wettbewerb spielen zu lassen. Das muss nicht heissen, alles doppelt aufzubauen, aber vielleicht nicht alles auf eine einzige Karte wie die Microsoft-Cloud zu setzen.

Und was die AI betrifft: Setzen Sie sie ein. Es gibt zwar einige technische Eigenheiten beim Aufsetzen und Nutzen von AI-Modellen, aber AI lässt sich meiner Erfahrung nach sicher und nutzbringend einsetzen. Steuern sollte dies jedoch das Unternehmen und es nicht den Mitarbeitenden überlassen, welche Tools sie etwa auf ihren privaten Mobilgeräten für die Zwecke der Arbeit einsetzen, weil der Arbeitgeber nichts Anständiges bietet. Den wirklichen Konkurrenzvorteil bringt die KI allerdings nicht denen, die die richtigen Tools haben, sondern denen, die an breiter Front verstehen, wie sie sich einsetzen lässt. Investieren sie nicht in technische Spielereien oder in das erstbeste Tool, das ihnen AI anbietet, sondern in AI-Werkzeuge, die besonders niederschwellig funktionieren und wirklich die Pain-Points der Mitarbeitenden adressieren. Wir setzen ein solches ein und konnten damit bereits nach kurzer Zeit zwei Drittel der Belegschaft gewinnen, Tendenz weiter steigend. Was ich so höre, ist das viel mehr als bei unseren Mitbewerbern, auch jenen, mit teuren Legal-Tech-Lösungen. Da wir AI in einem Pay-as-go-Modell nutzen, haben wir minime laufende Kosten und alles macht so geschäftlich sofort Sinn. Und das sollte auch bei AI so sein, finde ich.

**René Schmidli:** David, herzlichen Dank für das Gespräch.

**David Rosenthal:** Ich danke dir und vor allem den Verwaltungsräten, die sich dieser anspruchsvollen, aber strategisch zentralen Fragestellung aktiv annehmen.