INSTITUT FÜR COMPLIANCE UND WHISTLEBLOWING

Konferenzbericht

5. Konferenz

«Compliance – Whistleblowing – Corporate Governance»

5. November 2025 in Zürich

Konferenzleitung und Moderatoren

Prof. Dr. Patrick Krauskopf, LL.M.

- Professor
- Rechtsanwalt
- Ehemaliger Vizedirektor Wettbewerbskommission Schweiz

Dr. Rolf Raum

- Of Counsel Compliance Rechtsanwälte
- Ehem. Vorsitzender Richter 1. Strafsenat Bundesgerichtshof i.R.
- Vorsitzender ICW-Beirat

Patrick Wellens

- Global Compliance Business Partner
- Vorsitzender Ethics and Compliance Switzerland

Speakerinnen und Speaker

Prof. Dr. Jörn Basel

- Professor Wirtschaftspsychologie, Hochschule Luzern HSLU
- Advisor und Co-Partner The Negotiation Studio

Prof. Dr. Thomas Berndt

- Professor für Rechnungslegung, Universität St.Gallen HSG
- Direktor Institut für Law & Economics (ILE-HSG)

Manuela Broz

- Führung und Kulturberatung

Mona Fahmy

- CEO AGON COMPLIANCE AG

lic. iur. Samantha Fedeli

- Advokatin
- Chief Compliance Officer BKW

Tobias Gurtner

- CEO AGON INNOVATION AG
- Experte Cyber-Sicherheit und KI

Dr. Firas Nadim Habach, CFA

- Swiss Head of Financial Crime Compliance Central Europe Revolut

Prof. Dr. Christian Hauser

- Professor Betriebswirtschaftslehre, Fachhochschule Graubünden FHGR

Prof. Dr. Stefan Hunziker

- Professor Risk Management, Hochschule Luzern HSLU

Kaisa Karvonen

- Leiterin Forensic Services BDO Schweiz

Dr. Fabian Teichmann

- CEO Teichmann International AG
- Rechtsanwalt

Begrüssung durch Prof. Dr. Patrick Krauskopf und Dr. Rolf Raum

Die Konferenz startete mit der Begrüssung durch den Institutsvorsitzenden Dr. Rolf Raum und Prof. Dr. Patrick Krauskopf, die alle Teilnehmenden sowie Speakerinnen und Speaker herzlich willkommen hiessen. Dabei betonten sie die Bedeutung des Themas Compliance für die Praxis. Die Eröffnung setzte den Rahmen für die folgenden Vorträge und Diskussionen und unterstrich die Relevanz empirischer Forschung für die Umsetzung in der Praxis.

Alle in diesem Bericht wiedergegebenen Aussagen und Ausführungen erfolgen ausschliesslich in privater Funktion und stellen persönliche Meinungen dar. Sie sind nicht als offizielle Stellungnahmen des jeweiligen Berufs, Unternehmens oder der Behörde zu verstehen.

Einstiegsreferat lic. iur. Samantha Fedeli «Compliance – einfach… genial»

Samantha Fedeli stieg damit in die Konferenz ein, «dass Compliance keine Raketenwissenschaft ist», sie müsse einfach, praktikabel und alltagstauglich gestaltet werden. Komplexität entstehe häufig unnötig, insbesondere in gewissen Rechtskulturen. Ihr Anliegen ist es, Compliance zugänglich zu machen und ihre Bedeutung als Schutzfunktion für Unternehmen wie für Mitarbeitende sichtbar zu machen.

Fedeli blickt auf rund 15 Jahre Erfahrung zurück und stellte fest, dass die Regulierung stark zugenommen hat, insbesondere für kleine und mittlere Unternehmen, die sich oft schwertun, die Anforderungen umzusetzen. Gerade deshalb brauche es einfache, aber wirksame Ansätze.

Im Kern gehe es bei Compliance um Risiken und Prävention. Unternehmen dürften und müssten Risiken eingehen, aber innerhalb klarer Grenzen. Compliance unterstütze dabei, gesetzliche Vorgaben, interne Regeln und ethische Standards einzuhalten. Mit dem wachsenden Fokus auf ESG erhielten ethische Aspekte zusätzliches Gewicht. Richtig umgesetzt stärkt Compliance die Rechtssicherheit, das Vertrauen der Stakeholder und die Wettbewerbsfähigkeit, besonders für Schweizer Unternehmen, die international tätig sind. Zudem schützt sie vor rechtlichen Konsequenzen und hohen finanziellen Schäden.

Fedeli hob drei zentrale Erfolgsfaktoren hervor:

1. Klarheit der Regeln: Sie müssen zum Unternehmen passen und pragmatisch anwendbar sein.
2. Einbindung der Mitarbeitenden und Führungskräfte: Führungspersonen sind zentrale Multiplikatoren. Werden Compliance-Ziele in deren Verantwortung verankert, steigt die Wirksamkeit erheblich.
3. Vertrauenskanäle und Speak-Up-Kultur: Hinweisgebersysteme seien essenziell. Mitarbeitende müssen ohne Angst vor Sanktionen Missstände offen ansprechen können. Nur so entsteht eine Kultur, in der «rosarote Elefanten» nicht ignoriert, sondern proaktiv adressiert werden.

Abschliessend hob Samantha Fedeli die Wichtigkeit hervor, dass jedes Unternehmen über Compliance sprechen müsse: Sie schützt, stärkt und rechnet sich langfristig immer. Gleichzeitig ist Compliance ein kontinuierlicher Verbesserungsprozess, der ständiges Hinterfragen und Weiterentwickeln verlangt, vergleichbar mit einem Sicherheitsgurt: «den man hoffentlich nie braucht, aber dennoch unverzichtbar ist».

Für die Unterlagen zum Inputreferat besuchen Sie unsere Webseite icw-dach.com (Konferenzen > Konferenzen 2025 > 5. Konferenz Zürich 05.11.2025 > Powerpoint-Präsentation Samantha Fedeli).

Zweites Inputreferat von Prof. Dr. Jörn Basel «Compliance-check mittels KI – Easier said than done?»

In seinem Inputreferat widmete sich Prof. Dr. Jörn Basel der Frage, inwiefern präventive Compliance-Arbeit durch einen KI erleichtert werden kann. Zur Verdeutlichung führte er mit einem kurzen Videobeispiel in das Thema ein: Die Teilnehmenden sollten sich in die Rolle von Compliance-Verantwortlichen versetzen und prüfen, ob das gezeigte Werbe-Video, einer internen Freigabe standhalten würde. Die Zusammenarbeit zwischen Unternehmen und Influencerinnen und Influencer kann problematisch sein, da Content Creator Externe sind, die sich auch an die ethischen Standards des Unternehmens zu halten haben. Nun stellte er die Frage, wie sichergestellt werden kann, dass Compliance Richtlinien auch hier eingehalten werden und ob es KI-gestützte Tools gibt, die prüfen, ob so ein Video in den ethischen Rahmenbedingungen des Unternehmens fällt.

Im Anschluss wurde diskutiert, inwieweit technische Lösungen, insbesondere KI-gestützte Bewertungstools, Unternehmen künftig bei der Prüfung von Werbe- und Kommunikationsinhalten unterstützen können. Prof. Dr. Basel betonte, dass die Kombination aus rechtlichen Standards, klaren Kriterien und maschineller Auswertung durchaus Potenzial biete, allerdings nur als Ergänzung menschlicher Expertise: «KI sollte ein Sparringspartner sein: flankierend, nicht substituierend.» Eine vollständige Automatisierung sei weder realistisch noch wünschenswert.

Besondere Aufmerksamkeit erhielt die Frage, wie sich der Einsatz solcher Tools auf die Kompetenzentwicklung von Influencern und Mitarbeitenden auswirkt. Mehrere Teilnehmende äusserten die Sorge, dass die ausschliessliche Optimierung von Inhalten „bis das Tool auf Grün springt“ langfristig zu einem Verlust kritischen Denkens führen könnte. Prof. Dr. Basel bestätigte diese Befürchtungen und verwies auf ähnliche Diskussionen in der Hochschullehre, wo bereits beobachtet werde, dass Studierende durch KI-gestützte Systeme grundlegende Reflexions- und Transferfähigkeiten verlieren könnten. Der gleiche Effekt drohe im Compliance-Umfeld, wenn Verantwortliche Entscheidungen zunehmend an Algorithmen delegierten.

Basel plädierte dafür, KI-basierte Systeme ausschliesslich als Unterstützung einzusetzen: als zusätzliche Perspektive, die ein Vier-Augen-Prinzip erweitert, aber niemals ersetzt. Die Entscheidungs- und Denkverantwortung müsse klar bei den Menschen bleiben. Nur so lasse sich verhindern, dass Lern- und Verantwortungsprozesse verflachen und dass Compliance in Zukunft auf automatisierte Routineprüfungen reduziert wird.

Paneldiskussion: «Compliance und Whistleblowing unter der Lupe der Empirie» mit Mona Fahmy, Prof. Dr. Christian Hauser und Prof. Dr. Stefan Hunziker, moderiert von Prof. Dr. Patrick Krauskopf

In der ersten Paneldiskussion standen zwei Studien im Fokus, der Whistleblowing Report 2025 und Return on Compliance. Prof. Dr. Hauser und Prof. Dr. Hunziker stellten die Studien jeweils kurz vor und Mona Fahmy, Expertin in Economic Crime Investigation und ehemalige Investigativjournalistin, stellte daraufhin wichtige und kritische Fragen.

Whistleblowing Report

Prof. Dr. Christian Hauser stellte zu Beginn, den im September veröffentlichten Whistleblowing Report vor. Dabei präsentierte er die Ergebnisse der internationalen Vergleichsstudie. Während sich die wissenschaftliche Diskussion häufig darauf konzentriert, warum Individuen zu Whistleblowern werden, ein Thema, das eher in der Wirtschaftspsychologie verortet ist, richtet sich dieser Forschungsstrang auf die organisatorische Ebene: Wie setzen Unternehmen Hinweisgeber- und Beschwerdemechanismen praktisch um, und welche Wirkung entfalten diese Systeme?

In der Studie wurden insgesamt 2’200 Unternehmen in sieben Ländern befragt. Etwa ein Drittel der befragten Unternehmen zählt zu den KMU, zwei Drittel zu Grossunternehmen. Die Untersuchung zeigt, dass Meldestellen und externe Beschwerdekanäle in vielen Ländern mittlerweile weit verbreitet sind. Rund zwei Drittel der Unternehmen verfügen über entsprechende Strukturen, wobei häufig sowohl interne Meldestellen als auch externe Beschwerdesysteme parallel existieren. Besonders früh war hier die Schweiz, deren Finanzindustrie massgeblich zur Etablierung professioneller Whistleblowing-Kanäle beigetragen hat.

Auffällig ist jedoch, dass Schweizer Unternehmen im internationalen Vergleich an Dynamik verlieren. Während sie bei früheren Erhebungen in mehreren Bereichen führend waren, liegen sie heute beim Anteil relevanter Meldungen im Mittelfeld. Zudem ist der Anteil als missbräuchlich eingestufter Fälle gestiegen. Eine Entwicklung, die Prof. Dr. Hauser selbst überraschte, da die Schweiz über Jahre hinweg konstant die niedrigsten Werte aufwies. Trotzdem könne man nicht davon ausgehen, dass die Möglichkeit anonymer Meldungen zu mehr missbräuchlichen Hinweisen führt, was ein häufig geäussertes, jedoch empirisch unbegründetes Vorurteil ist.

Prof. Dr. Hauser warnte davor, diese Entwicklung vorschnell zu überinterpretieren. Da es sich nicht um eine Panel-Studie handelt, lassen sich die Ergebnisse nicht direkt 1:1 vergleichen. Dennoch spricht er von einem klaren Trend: Unternehmen in der Schweiz scheinen ihre Meldesysteme weniger aktiv zu pflegen als früher. Dies könne die Qualität und Relevanz der eingehenden Hinweise beeinträchtigen.

Er stellte daher die Frage in den Raum, ob strukturelle Aspekte, wie nachlassende Kommunikation, mangelnde Schulung oder reduzierte Pflege der Systeme, zu diesem Rückgang beitragen könnten. Die Dringlichkeit weiterer Forschung sei offensichtlich, insbesondere um zu verstehen, ob kulturelle oder organisatorische Veränderungen hinter diesen Entwicklungen stehen.

Mona Fahmy äusserte sich positiv zum Report, er leiste einen wichtigen Beitrag zur Compliance-Prävention und liefert Vergleichszahlen. Die Studie gebe Frühwarnsystemen und Hinweisgeberschutz neue Substanz und zeige den Nutzen von Meldestellen auf. Trotzdem stellte sie kritische, aber wichtige, Fragen: Wie wurde überprüft, ob Missstände korrekt erfasst wurden und ob Missbrauch oder Fehlinterpretationen vorliegen? Fahmy fragt, ob Unternehmensangaben verlässlich sind, ob Missstände eventuell unvollständig erfasst wurden und ob missbräuchliche Meldungen möglicherweise überinterpretiert wurden. Prof. Dr. Hauser antwortete, dass die Studie klare Aussagen zur Missbrauchsquote liefert. Es gibt keinen empirischen Zusammenhang zwischen anonymen Meldungen und Missbrauch: «Wir haben in keiner unserer Studien einen Zusammenhang zwischen anonymen Meldungen und einer höheren Missbrauchsquote gefunden.». Die Schweiz weist erstmals einen deutlichen Anstieg missbräuchlicher Fälle auf, liegt aber weiterhin im niedrigeren Bereich. Die Ursache ist nicht auf Überinterpretationen der Befragten zurückzuführen, sondern deutet eher auf organisatorische Gründe, z. B. Systeme werden weniger gepflegt, Verantwortlichkeiten werden nicht mehr so aktiv wahrgenommen, der Betrieb der Meldestellen verliert an Dynamik. Weiter fragt Mona Fahmy: «Hinken Schweizer Unternehmen wirklich hinterher oder liegen kulturelle Unterschiede oder fehlerhafte Interpretationen zugrunde?» Laut Hauser habe die Schweiz in früheren Erhebungen geführt, verlor aber jetzt deutlich an Dynamik. Die Rückgänge sind wahrscheinlich nicht kulturell bedingt, da die Befragten zuvor über Jahre hinweg konsistente Werte ablieferten. Die plausibelste Erklärung sei organisatorisch: „…dass diese Systeme mittlerweile doch auch weniger gepflegt werden als früher.“ Ein kultureller Erklärungsansatz wird somit eher ausgeschlossen.

Zum Schluss stellt Fahmy die Frage in die Runde, welche Bedeutung Anonymität für die Qualität und Nutzung von Meldungen habe. Die Panelistin zweifelte, ob Mitarbeitende sich tatsächlich trauen, Missstände offen zu melden, und fragt nach Qualitätskriterien für anonyme Hinweise. Die Studie zeige aber,

dass Anonymität wichtig ist, aber nicht problematisch. Anonyme Kanäle führen nicht zu mehr Missbrauch. Die Schweiz liegt bei der Möglichkeit anonymer Meldungen im Durchschnitt der untersuchten Länder und die Aussagekraft der Meldungen hängt nicht davon ab, ob sie anonym erfolgen.

Return on Compliance

Die Frage nach dem messbaren Wert von Compliance für Unternehmen gehört zu den zentralen, bisher jedoch wenig empirisch untersuchten Themen im Bereich Unternehmensführung. Die Studie *Return on Compliance* hat diese Lücke adressiert, indem sie systematisch untersucht, ob und wie Compliance einen messbaren Beitrag zum Unternehmenserfolg leistet.

Die Ausgangslage war eindeutig: Unternehmen investieren heute historisch hohe Summen in Compliance, doch empirisch konnte bisher nicht gezeigt werden, ob diese Ausgaben tatsächlich einen Return erzeugen. Formale Compliance-Massnahmen wie Policies, Regeln oder Dokumentationen allein reichen offenbar nicht aus, um messbare Effekte zu erzielen. Ziel der Studie war daher, die Wirksamkeit von Compliance empirisch zu prüfen und die zentralen Treiber für erfolgreichen Compliance-Einsatz zu identifizieren.

Die Ergebnisse zeigen klar, dass es drei entscheidende Erfolgsfaktoren für Compliance gibt, die nicht kompensierbar sind:

1. Compliance muss einen Sitz am Entscheidungstisch haben, also aktiv und frühzeitig in Entscheidungsprozesse eingebunden sein.
2. Die systemische Compliance-Kompetenz ist entscheidend, sowohl auf Seiten des Managements als auch der Compliance-Abteilungen.
3. Die Anpassungsfähigkeit spielt eine zentrale Rolle: Compliance muss in der Lage sein, schnell auf externe regulatorische Änderungen sowie interne Anpassungen von Geschäftsmodellen und Strategien zu reagieren.

Darüber hinaus konnten weitere relevante Faktoren identifiziert werden, die den Erfolg von Compliance unterstützen, aber weniger stark wirken. Dazu gehören Legitimität und soziale Sicherheit innerhalb des Unternehmens sowie die Unternehmenskultur. Formalistische Compliance-Massnahmen allein, also das Vorhandensein von Regeln oder Dokumentationen, reichen hingegen nicht aus, um das Verhalten von Mitarbeitenden nachhaltig zu verändern.

Die Studie liefert damit wichtige Implikationen für die Praxis: Compliance sollte nicht als formale Pflichtaufgabe verstanden werden, sondern als strategischer Erfolgsfaktor, der aktiv in Entscheidungen eingebunden ist. Investitionen in Compliance zahlen sich insbesondere dann aus, wenn sie Kompetenz, Einfluss und Anpassungsfähigkeit fördern. Auf Grundlage der Ergebnisse wurde zudem ein praxisnahes Monitoring- und Steuerungsmodell entwickelt, das es Unternehmen ermöglicht, den Wert von Compliance messbar zu machen.

Auch hier stellte Mona Fahmy wieder eine kritische Frage: „Die meisten Schweizer Unternehmen sind KMU. Diese haben nicht die gleichen Möglichkeiten wie Grossunternehmen – sind sie möglicherweise überfordert, die Ergebnisse der Studie umzusetzen?“. Prof. Dr. Hunziker antwortete, dass die Studie zeige, dass Compliance-Kompetenz nicht primär an die Grösse des Unternehmens oder an spezielle Abteilungen gebunden ist, sondern systemisch verstanden werden muss. Entscheidend ist, dass Management und Mitarbeitende die Relevanz von Compliance für den Geschäftserfolg erkennen, eine entsprechende Awareness entwickeln und Compliance als integralen Bestandteil der Unternehmenskultur verankern.

Interessanterweise hätten KMU hier oft sogar Vorteile: Compliance ist näher am Tagesgeschäft, und Entscheidungen werden direkt unter Einbezug von Compliance-Aspekten getroffen. Entscheider „haben Skin in the Game", wodurch die Umsetzung von Compliance-Massnahmen unmittelbar und praxisnah erfolgt. Ressourcenknappheit oder kleinere Strukturen bedeuten nicht automatisch geringere Wirksamkeit. Die Studie zeigte, dass gerade inhabergeführte Unternehmen durch diese direkte Einbindung oft besonders effektive Compliance-Praktiken entwickeln können.

Die Ergebnisse verdeutlichen damit, dass die Umsetzung der Erkenntnisse nicht auf Grossunternehmen beschränkt ist. KMU sind durchaus in der Lage, die Prinzipien der Studie erfolgreich in ihrer Organisation zu integrieren.

Drittes Inputreferat von Dr. Firas Nadim Habach, CFA «FinTechs im Spannungsfeld von Skalierbarkeit und Nachhaltigkeit: Moderne Ansätze zur Bekämpfung von Finanzkriminalität»

Ausgangspunkt des Inputreferats von Dr. Habach war der enorme Skalierungsdruck, dem FinTechs ausgesetzt sind. Revolut verzeichnete in der Schweiz innerhalb kurzer Zeit ein starkes Wachstum und explodierende Nutzerzahlen. Dieses Wachstum stellt die Compliance-Funktion vor besondere Herausforderungen: Traditionelle Verfahren klassischer Banken, etwa manuelle oder papierbasierte Prüfprozesse, sind mit solchen Volumina nicht vereinbar. FinTechs müssen daher auf moderne, skalierbare technische Lösungen setzen, ohne dabei an regulatorischer Sorgfalt einzubüssen.

Habach betonte, dass viele etablierte Banken technologisch noch immer mit veralteten Kernbanksystemen arbeiten, während FinTechs deutlich schneller neue regulatorische Anforderungen integrieren können. Gleichzeitig sei Technologie kein vollständiger Ersatz für menschliche Expertise. Entscheidend bleibe die Kombination aus leistungsfähigen Systemen, qualifizierten Fachpersonen und der Fähigkeit, sich laufend anzupassen. Proaktivität statt reiner Reaktion sei dabei ein zentrales Prinzip nachhaltiger Compliance-Arbeit.

Im Bereich der Finanzkriminalitätsbekämpfung eröffnen neue digitale Angebote zusätzliche Datenquellen, etwa durch die Nutzung von E-SIMs oder technischen Standortinformationen. Diese können helfen, die Plausibilität von Kundendaten zu prüfen und verdächtige Aktivitäten frühzeitig zu erkennen.

Ein weiterer Fokus lag auf der steigenden Belastung der Meldestellen. Der Referent verwies auf deutliche Zuwächse bei Verdachtsmeldungen, nicht nur bei FinTechs, sondern branchenweit. Der wachsende Druck auf Aufsichtsbehörden und Banken mache effiziente technische Lösungen unerlässlich. Gleichzeitig zeige sich, dass manche der grössten Betrugsfälle nicht aus dem FinTech-Bereich stammten, sondern aus traditionellen Institutionen, denen oftmals die Datenbasis fehle, um bestimmte Muster zu erkennen.

Abschliessend fasste Dr. Firas Habach zusammen, dass trotz fortschrittlicher Technologien menschliche Urteilsfähigkeit unverzichtbar bleibt. Die besten Ergebnisse entstehen dort, wo Datenintelligenz, technische Skalierbarkeit und erfahrene Compliance-Teams zusammenwirken.

Viertes Inputreferat von Kaisa Karvonen «Hinweisen Gehör verschaffen: Wie KMU durch Whistleblowing Compliance stärken»

Kaisa Karvonen zeigte gelungen auf, welche zentrale Rolle Whistleblowing-Systeme für die Betrugsbekämpfung und die Stärkung von Compliance spielen, insbesondere für kleine und mittlere Unternehmen. Die Referentin verfügt über langjährige Erfahrung im Bereich Forensic Accounting und der Untersuchung von Betrugs- und Fälschungsfällen und brachte zahlreiche Erkenntnisse aus der Praxis ein.

Anhand zweier Fallbeispiele wurde deutlich, wie entscheidend funktionierende Hinweisgebersysteme sind. Im ersten Fall bemerkte eine Mitarbeiterin Unregelmässigkeiten in einem Logistiklager. Obwohl sie diese ihrem Vorgesetzten meldete, wurde das Problem ignoriert, und aus Angst vor Repressalien sah sie von weiteren Schritten ab. Erst später wurde klar, dass dem Unternehmen ein Schaden von mehreren Millionen Franken entstanden war.

Ein zweites Beispiel aus dem öffentlichen Sektor zeigte, wie fehlende Meldemöglichkeiten dazu führen können, dass Unregelmässigkeiten in Vergabeverfahren unentdeckt bleiben. Beide Fälle verdeutlichen, wie wichtig sichere und vertrauenswürdige Meldekanäle sind.

Die Referentin erläuterte anschliessend, welche typischen Phasen ein Whistleblowing-Fall in Organisationen durchläuft, von der Meldung über die Ersteinschätzung bis zur Untersuchung und anschließenden Maßnahmen.

Besonders wichtig ist die Möglichkeit, Hinweise anonym abzugeben. Statistisch zeigt sich, dass zwar über 90 Prozent der Mitarbeitenden Missstände melden möchten, tatsächlich aber nur etwa die Hälfte dies tun. Die häufigsten Gründe für unterlassene Meldungen sind die Angst vor Vergeltungsmassnahmen sowie Zweifel daran, dass ihre Meldung überhaupt zu Konsequenzen führt. Ein verlässliches, anonymes System erhöht nachweislich die Anzahl und Qualität der Hinweise.

Whistleblowing-Systeme sind unabhängig von Unternehmensgrösse oder Branche wirksam. Jede Organisation muss jedoch definieren, welche Arten von Meldungen aufgenommen werden sollen – ob ausschliesslich Compliance- und Integritätsthemen oder auch allgemeine Prozess- und Arbeitsplatzbeschwerden. Für KMU bieten solche Systeme einen besonderen Mehrwert: Sie stellen eine kostengünstige und sehr effektive interne Kontrolle dar, die auch Risiken adressiert, die sich sonst kaum überwachen lassen, etwa das Überschreiben von Kontrollen durch das Management. Whistleblowing ist damit eines der stärksten Instrumente zur Betrugsprävention und ein zentrales Element moderner Compliance-Strukturen.

Abschliessend betonte Kaisa Karvonen, dass funktionierende Hinweisgebersysteme entscheidend sind, um Transparenz, Vertrauen und eine robuste Compliance-Kultur im Unternehmen zu fördern.

Für einen Einblick in die Folien des Inputreferats von Kaisa Karvonen besuchen Sie unsere Webseite icw-dach.com (Konferenzen > Konferenzen 2025 > 5. Konferenz Zürich 05.11.2026 > Powerpoint-Präsentation Kaisa Karvonen).

Paneldiskussion «Corporate Governance Herausforderungen 2026» mit Manuela Broz, Prof. Dr. Thomas Berndt, Dr. Fabian Teichmann, moderiert von Patrick Wellens

Der Moderator Patrick Wellens warf zunächst die Frage auf, warum trotz umfangreicher Compliance-Prozesse in vielen Unternehmen weiterhin gravierende Skandale auftreten. Manuela Broz führte aus, dass der entscheidende Faktor weniger im Regelwerk selbst liege, sondern in der gelebten Unternehmenskultur. Diese Kultur sei ein Spiegel dessen, was im Unternehmen tatsächlich akzeptiert werde und damit Ausdruck der täglichen Entscheidungs- und Verhaltensmuster. Regeln allein reichten nicht aus, betonte sie. „Kultur ist Integrität in der Umsetzung“, und genau an dieser Umsetzung scheitere es häufig. Zwar sei bekannt, was notwendig wäre, doch unter realen Arbeitsbedingungen wie Zeitdruck, ständige Unterbrechungen, hohe Erwartungen und vielfältige Belastungen, fehle oft der Raum, um sich im Team mit ethischen Fragen auseinanderzusetzen.

Im weiteren Verlauf wurde diskutiert, wie „Tone from the Top“, Leitbilder und Codes of Conduct tatsächlich wirksam werden können. Es reiche nicht, Werte zu definieren, wenn beispielsweise keine angemessenen Budgets bereitgestellt würden oder Führungskräfte selbst kein Vorbild seien. Daher stellte

sich die Frage nach konkreten Parametern, an denen eine funktionierende Kultur erkennbar sei. Broz argumentierte, dass Appelle wie „Vertrauenskultur schaffen“ ins Leere liefen. Vertrauen entstehe nicht durch Worte, sondern durch strukturelle Bedingungen. Menschen verhielten sich so, wie es der Kontext nahelege, deshalb müsse dieser Kontext gestaltet werden. Kultur sei letztlich „knallharte Strukturarbeit“ und funktioniere wie ein Betriebssystem des Unternehmens. Broz führte die Stop-Kriterien ein: *Was im Unternehmen nicht bewusst gestoppt wird, setzt sich automatisch fort und oft mit gravierenden Folgen.* Stop-Kriterien sind deshalb ein zentrales Werkzeug, um Risiken zu vermeiden, kritisches Denken zu fördern und eine Kultur zu schaffen, in der Mitarbeitende sich trauen, Verantwortung zu übernehmen.

Als Beispiel für den Aufbau einer Speak-Up-Kultur nannte Manuela Broz, neuen Mitarbeitenden bereits am ersten Tag die Aufgabe zu geben, Beobachtungen, inklusive kritischer Punkte, festzuhalten und diese im Rahmen eines Gesprächs einzubringen. Speak-Up beginne dort, wo Mitarbeitende Verantwortung übernehmen dürfen und ihre Autonomie gestärkt werde. Dazu gehöre auch, dass Führungskräfte Widerspruch aushalten könnten und ihn als Beitrag zur Leistungssteigerung verstünden.

Broz schloss mit dem Hinweis, dass echte kulturelle Transformation arbeitsintensiv sei, sich jedoch als Investition in die Zukunftsfähigkeit des Unternehmens lohne. Sie begleite Organisationen, die diesen Weg einschlagen, und sehe dort, wie wirkungsvoll konsequente Strukturarbeit sein könne.

Zum Schluss stelle Patrick Wellens die Frage, wie Unternehmen die richtige Balance zwischen Strukturen und Kontrollmechanismen sowie echter Eigenverantwortung der Mitarbeitenden finden, sodass Compliance-Anforderungen erfüllt werden, aber auch die Mitarbeitenden motiviert bleiben, Probleme selbst zu lösen. Darauf antwortete Manuela Broz mit: «Menschen sind motiviert. Und wenn sie es nicht mehr sind, hat man sie demotiviert.». In vielen Unternehmen könnten Mitarbeitende ihre Autonomie nicht leben, was zu Frustration und Leistungsverlust führe. Sie verwies auf eine verbreitete Praxis in ihren Kundenprojekten: Probleme sollten stets dort gelöst werden, wo sie entstehen, denn dort liege die entsprechende Kompetenz. Es sei wenig sinnvoll, dass sich das Top-Management mit operativen Detailproblemen befasse, die es weder kenne noch fachlich beurteilen könne. Hinter solchen Fehlallokationen stünden oft Machtthemen.

Im weiteren Verlauf des Panels wurde die Rolle von Künstlicher Intelligenz (KI), Corporate Governance und den damit verbundenen Anforderungen an Vorstände und Verwaltungsräte diskutiert. Ausgangspunkt war die Frage, wie Unternehmen sicherstellen können, dass KI-Anwendungen verantwortungsvoll genutzt werden und wie sich dies auf Kultur, Risiko und Führung auswirkt.

Dr. Fabian Teichmann betonte zunächst, dass die theoretische Debatte häufig sehr abstrakt geführt werde, mit Begriffen wie „Transparenz“, „Blackbox-Vermeidung“ oder umfassenden Regulierungsmodellen. In der Praxis seien die Herausforderungen jedoch oftmals viel einfacher: Organisationen müssten lernen, den Umgang mit neuen Technologien konsequent zu schulen. Der jüngste Fall einer KI-generierten CEO-Stimme, die Mitarbeitende zur Überweisung hoher Beträge verleitet hatte, sei weniger ein technologisches, sondern vor allem ein Schulungsdefizit.

Vorstände und Verwaltungsräte müssten sich daher eine zentrale Frage stellen: Haben wir im obersten Entscheidungsgremium überhaupt die Expertise, diese Technologien zu verstehen und zu überwachen? Wenn dies nicht der Fall sei, müsse gezielt Know-how hinzugezogen oder in den Verwaltungsrat integriert werden.

Teichmann verwies auf die zunehmende Regulierungsdichte. Diese Themen seien hochkomplex und erforderten Personen, die sowohl juristisch als auch technisch denken könnten. Allein auf Techniker zu

setzen, sei ebenso unzureichend wie ein rein juristischer Blick. Erst die Kombination beider Perspektiven ermögliche verantwortungsvolle Steuerung.

Ein weiteres Thema war die Cybersecurity, insbesondere in komplexen Lieferketten mit hunderten oder tausenden Zulieferern. Führungsgremien sollten sich mit der Frage befassen: Wie würden wir unser eigenes Unternehmen angreifen, wenn wir Hacker wären? Diese Perspektive schärfe das Bewusstsein für reale Schwachstellen, auch jenseits der üblichen Testverfahren. Viele Firmen, die sich selbst nicht als typische Angriffsziele betrachteten, beispielsweise Steuerberater, Wirtschaftsprüfer, Buchhaltungs- oder Anwaltskanzleien, seien in Wahrheit besonders exponiert: wertvolle Daten, vergleichsweise geringe IT-Budgets und hohe Abhängigkeit von Vertraulichkeit machten sie attraktiv für Angreifer. Teichmann schilderte ein Beispiel aus der Praxis: Bei kleinen und mittleren Unternehmen könne es vorkommen, dass ein Angreifer alle Daten verschlüssele, ein Lösegeld fordere und gleichzeitig über Backups verfüge. Die Drohung, sensible Daten schrittweise zu veröffentlichen, könne innerhalb weniger Tage existenzielle Krisen auslösen.

Gerade deshalb sei es entscheidend, dass Unternehmen, grosse wie kleine, ihre Cyberstrategie überdenken, Szenarien realistisch durchspielen und sowohl technische als auch organisatorische Schutzmechanismen stärken.

Der dritte Panelist Prof. Dr. Thomas Berndt verwies auf das weit verbreitete Modell der *Three Lines of Defense*, das in der Vergangenheit zwar wertvolle Dienste geleistet habe, aber zugleich ein ausgeprägtes Silodenken begünstigt habe. Dieses führe zu organisatorischen Fehlallokationen: Jede Linie arbeite mit eigenen Tools, eigenen Prozessen und eigenen Prioritäten, wodurch Schnittstellenprobleme, Koordinationsaufwand und Effizienzverluste entstünden. Gerade aus Governance-Perspektive seien solche Fragmentierungen problematisch. Deshalb gewinnen integrierte Ansätze zunehmend an Bedeutung. Der genaue Begriff sei dabei unerheblich; entscheidend sei das Prinzip eines koordinierten Vorgehens entlang einer gemeinsamen Risikobereitschaft des Unternehmens. Warum dieser Wandel gerade jetzt so wichtig ist, erläuterte der Panelist anhand aktueller Risikobewertungen. Globale Risiko-Reports, darunter auch bekannte Wirtschafts-Surveys, zeigten ein verändertes Bild: Unter den Top-Risiken befänden sich nicht mehr primär finanzielle Themen, sondern Misinformation und Disinformation, extreme Wetterereignisse und geopolitische Konflikte. Diese Veränderungen stellten die Frage, ob Governance- und Assurance-Systeme, die stark auf finanzielle Kennzahlen ausgerichtet sind, heutigen Realitäten noch gerecht werden.

Parallel dazu habe sich die „Risk Landscape“ deutlich beschleunigt und sei wesentlich volatiler geworden. Viele Mitglieder der heutigen Managementebenen hätten ihre berufliche Sozialisation in vergleichsweise stabilen Zeiten erlebt, eine Herausforderung, wenn heute Investitionsentscheidungen mit 30-jährigen Amortisationshorizonten unter Bedingungen permanenter Unsicherheit getroffen werden müssten. Governance-Anforderungen hätten sich entsprechend grundlegend gewandelt.

Auf die Frage, wie Unternehmen angesichts dieser Dynamik praktikable Steuerungsmechanismen gestalten können, verwies der Panelist auf zwei pragmatische Kernaspekte:

1. Der Mismatch zwischen kurzfristigen Entscheidungen und langfristigen Wirkungen

Viele Massnahmen, wie ESG-relevante Investitionen oder Transformationsprojekte, erzeugen kurzfristig Kosten, entfalten ihre positiven Effekte aber erst nach 15 bis 20 Jahren. Dies erschwert Governance-Entscheidungen und erzeugt Reibungen innerhalb der Organisation.

2. Unterschiedliche Daten- und Reportinggrundlagen

Ein wesentlicher Teil des Problems liege darin, dass verschiedene Bereiche mit unterschiedlichen Daten, Kennzahlen und Reporting-Logiken arbeiten. Externes Rechnungswesen, internes Rechnungswesen, Compliance, ESG, Risk Management oder Finance lieferten jeweils eigene Reports. Dies führe zu widersprüchlichen Argumentationslinien und Konflikten in der Unternehmenssteuerung.

Der Panelist plädierte daher für eine einheitliche Datenbasis und integrierte Dashboards, auf deren Grundlage alle Funktionen entscheiden können. Erst durch ein solches gemeinsames Fundament werde ein wirklich integriertes Governance- und Assuranceverständnis möglich. Grosse Wirtschaftsprüfungsgesellschaften würden diesen Ansatz bereits propagieren; er sei jedoch noch längst nicht überall etabliert.

Interview mit Tobias Gurtner «Compliance neu denken im KI-Zeitalter –Tobias Gurtner über Cybersicherheit und globale Lieferketten» moderiert von Prof. Dr. Patrick Krauskopf

Patrick Krauskopf stieg mit der Opening Question zum Thema Governance im Zeitalter intelligenter Systeme ein. Tobias Gurtner stellte fest, dass Künstliche Intelligenz unternehmerische Entscheidungen grundlegend verändert. Genau deshalb darf sie nicht als technisches Experiment behandelt werden, sondern muss auf Ebene des Verwaltungsrats verankert sein. KI ist ein Governance-Thema. Entscheidend sind klare Verantwortlichkeiten, Transparenz über Daten und Modelle sowie Nachvollziehbarkeit durch Dokumentation und Tests. Wird KI zur Blackbox, verliert das Unternehmen die Kontrolle über Risiken, Reputation und Handlungsfähigkeit. Statt auf detaillierte Regulierung zu warten, sollten Unternehmen eigene Leitplanken setzen: saubere Daten, klar definierte Anwendungsfälle, strukturierte Freigabeprozesse und einen risikobasierten Ansatz. Der Einstieg sollte dort erfolgen, wo der Nutzen hoch und das Schadenspotenzial überschaubar ist. Regulierung wirkt dabei nicht als Bremse, sondern als Vertrauensanker für nachhaltige Innovation.

Eng verknüpft mit KI ist die Cybersicherheit. Tobias Gurtner sagt, Cyber- und Datenrisiken gehören aus der IT-Ecke heraus und müssen als Business-Continuity-Thema geführt werden. Ein integriertes Risikobild, das IT-, Lieferketten- und Reputationsrisiken zusammenführt, schafft Transparenz und ermöglicht gezielte Steuerung. Wer Cyber nur als Kostenfaktor sieht, zahlt später, operativ wie finanziell. Für den Verwaltungsrat bedeutet das neue Anforderungen: Mindestens ein Mitglied sollte über fundierte Cyber- und Datenkompetenz verfügen. Klare Strukturen, definierte Eskalationswege und regelmässige Krisenübungen stärken die Aufsicht. Aufgabe des VR ist nicht die Umsetzung, sondern die wirksame Steuerung durch Fragen, Verantwortlichkeiten und messbare Kennzahlen.

Bei der Frage danach, wo KI den grössten Mehrwert in Compliance schafft und wo sie an ihre Grenzen gelangt, antwortet Gurtner, dass KI grossen Mehrwert dort schafft, wo Informationsflut zum Risiko wird, wie bei Sanktions-, Medien- oder Risiko-Screenings. Klare Grenzen sind nötig bei schlechter Datenqualität, unklarer Verantwortung oder hochwirksamen Entscheidungen ohne menschliche Kontrolle. Denn KI beschleunigt nicht nur gute Prozesse, sondern auch Fehler.

Tobias Gurtners Fazit ist klar: Die Zukunft bietet Chancen für jene Unternehmen, die Innovation mit Verantwortung verbinden. Wer heute Governance, Sicherheit und Transparenz ernst nimmt, baut Vertrauen und Resilienz auf. Wer zögert, überlässt anderen die Kontrolle über Daten, Risiken und die eigene Zukunft.

Abschluss der Konferenz

Zum Abschluss der Konferenz dankte Prof. Dr. Patrick Krauskopf allen Referentinnen, Referenten und Teilnehmenden für ihren engagierten Beitrag und den offenen fachlichen Austausch. Die lebendigen

Diskussionen, Perspektiven und Fragen aus dem Publikum haben die Bedeutung des Themas eindrucksvoll unterstrichen.

Mit dem Hinweis auf die 8. Konferenz des ICW in Zürich am 4. November 2026, die gewonnenen Impulse in die eigene Praxis mitzunehmen, wurde die Veranstaltung offiziell beendet. Die Teilnehmenden verabschiedeten sich in kollegialer Atmosphäre, mit wertvollen Kontakten, neuen Denkanstössen und dem gemeinsamen Bewusstsein, dass Compliance weiterhin ein zentraler Bestandteil verantwortungsvoller Unternehmensführung bleibt.

Autorin: Hannah Wenger