INSTITUT FÜR COMPLIANCE UND WHISTLEBLOWING

Konferenzbericht

4. Konferenz

«Compliance – Whistleblowing – Corporate Governance»

22. Oktober 2025 in Frankfurt

Konferenzleitung und Moderatoren

Prof. Dr. Heribert Hirte

- Ehemaliger Bundestagsabgeordneter
- ICW-Beirat Deutschland

Prof. Dr. Patrick Krauskopf, LL.M.

- Professor
- Rechtsanwalt
- Ehemaliger Vizedirektor Wettbewerbskommission Schweiz

Prof. Christian Strenger

- Direktor Corporate Governance Institute Frankfurt School

Dr. Martin Weimann

- Rechtsanwalt
- Ombudsmann und Vertretung Whistleblower

Speakerinnen und Speaker

Julia Arbery, LL.M.

- Partner AlixPartners

Dr. Sophia Habbe

- Partner White & Case
- Head of Investigations Germany

Manuel Heinemann

- Kriminologe
- Bedrohungsmanagement und Prävention zielgerichteter Gewalt
- Experte für Amokprävention
- Lehrbeauftragter für Kriminalpsychologie und Gefahrenmanagement

RAin Nadine Jacobi

- Inhaberin Kanzlei Compliance Customized
- Rechtsanwältin
- Ombudsperson
- Certified Fraud Examiner
- Dozentin

Patrick Knittel

- Ombudsperson Hinweisgeberschutz
- Lehrbeauftragter
- Datenschutzbeauftragter

Dr. Bárbara Lessa

- Senior Audit Compliance/GBS Deutsche Post und DHL

Dr. Rolf Raum

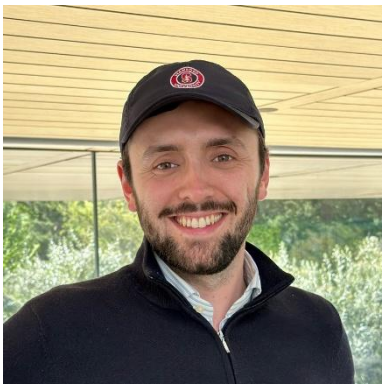
- Of Counsel Compliance Rechtsanwälte
- Vorsitzender Richter 1. Strafsenat Bundesgerichtshof i.R.
- Vorsitzender ICW-Beirat

Prof. Dr. Julia Redenius-Hövermann

- Professorin für Bürgerliches Recht und Unternehmensrecht
- Direktorin Corporate Governance Institute Frankfurt School

Dr. Mirjam Weisse

- Of Counsel Luther Rechtsanwaltschaftsgesellschaft



Paul Welter

- Rechtsanwalt
- CEO bayshore
- Adjunct Professor of Law Florida State University

Begrüssung durch Prof. Dr. Patrick Krauskopf und Prof. Christian Strenger

Zu Beginn der Veranstaltung begrüssten Prof. Dr. Patrick Krauskopf und Prof. Christian Strenger die Teilnehmenden herzlich zur vierten Konferenz des Instituts für Compliance und Whistleblowing. Sie betonten die ungebrochene Aktualität des Themas und freuten sich über die Beteiligung aller Speakerinnen und Speaker sowie Teilnehmenden. Krauskopf erläuterte die Zielsetzung der Tagung: Compliance nicht nur für Fachleute aufzubereiten, sondern ihre Bedeutung als gesellschaftlichen, volkswirtschaftlichen und betriebswirtschaftlichen Mehrwert aufzeigen. Die Konferenz solle damit einen Beitrag zur öffentlichen Debatte leisten und komplexe Inhalte verständlich vermitteln. Zugleich würdigte er die Expertise der eingeladenen Speakerinnen und Speaker. Abschliessend hob er die Bedeutung einer offenen, interaktiven Diskussion hervor und leitete in das Programm über.

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 RAin Nadine Jacobi «Nachgehen von Hinweisen und interne Untersuchungen im Kontext des HinSchG: Dos & Don'ts in der unternehmensinternen Praxis»

Das Einstiegsreferat hielt RAin Nadine Jacobi, Inhaberin einer Boutique Kanzlei in Hamburg, die auf Compliance und interne Untersuchungen spezialisiert ist. In Ihrem Inputreferat berichtete sie aus ihrer praktischen Erfahrung als Ombudsperson, Beraterin für Hinweismanagementsysteme sowie aus Krisen- und Interimsmandaten.

Auswahl und Einrichtung von Meldekanälen

Nadine Jacobi erläuterte die verschiedenen Möglichkeiten zur Implementierung eines Meldekanals: Ombudsperson, digitale Hinweismanagementsysteme oder hybride Modelle und erklärt, dass die Wahl des passenden Systems stark vom Unternehmenskontext abhängt. Grösse, Internationalität, bestehende Strukturen und Erfahrungen mit Vorgängermodellen bestimmen, welche Lösung geeignet ist. Seit Einführung des Hinweisgeberschutzgesetzes ist das *Ob* eines Meldesystems gesetzlich geklärt, das *Wie* bleibt jedoch anspruchsvoll. Unternehmen stehen vor der Aufgabe, Konzepte zu entwickeln, die sowohl funktional als auch organisationskulturell tragfähig sind.

Umgang mit Bedenken und kulturelle Herausforderungen

Jacobi berichtete, dass die Einführung eines Hinweisgebersystems häufig auf Vorbehalte stösst, etwa Sorgen vor Denunziation, Hinweisflut oder einer Störung der Unternehmenskultur. Besonders im Mittelstand und in familiengeführten Unternehmen seien diese Ängste verbreitet.

Sie empfiehlt, diese Bedenken ernst zu nehmen und ein durchdachtes Integrationskonzept zu entwickeln durch klare Kommunikation, Einbindung relevanter Stakeholder und Sensibilisierung für den Nutzen eines Meldesystems als Bestandteil einer gesunden Compliance- und Vertrauenskultur.

Praxis bei internen Untersuchungen

Ein Schwerpunkt des Vortrags lag auf der Untersuchung eingehender Hinweise. Nadine Jacobi schildert typische Herausforderungen, beispielsweise:

- Hinweise basieren häufig auf Hörensagen statt eigener Wahrnehmung.
- In einigen Fällen verfolgen Hinweisgeber oder Beteiligte eigene Agenden.
- Bei sensiblen Themen wie toxischen Führungskulturen oder Verhaltensverstössen gibt es oft nur wenige tatsächliche Zeugen.

Sie betonte deshalb die Bedeutung professioneller Interviewführung, hoher Sensibilität und genauer Analyse, insbesondere wenn nur subjektive Eindrücke statt Dokumente oder harte Fakten vorliegen. Anhand realer Beispiele, etwa Untersuchungen im Krankenhausumfeld oder dem Fall des Hamburger Balletts, zeigte sie, wie schnell Vorwürfe öffentliche Dynamik entfalten können und dass selbst unberechtigte Hinweise kaum einzufangen sind, sobald sie in den Medien stehen.

Empfehlungen und Fazit

Zum Abschluss fasste Nadine Jacobi zusammen, worauf Unternehmen bei der Einrichtung und dem Betrieb von Hinweisgebersystemen achten sollten:

- Passende Strukturwahl (Ombudsperson, digital, hybrid)
- Sensible Einführung und Kommunikation
- Schutz der Unternehmenskultur
- Professionelle Untersuchungspraxis
- Klare Abgrenzung dessen, was intern geleistet werden kann und wann externe Expertise notwendig ist

Nadine Jacobi schloss ihren Vortrag mit einem Dank und dem Hinweis, dass die bereitgestellten Folien die wichtigsten Punkte nochmals übersichtlich darlegen. Diese sind auf der Webseite des Instituts für Compliance und Whistleblowing zu finden (icw-dach.com > Konferenzen > Konferenzen 2025 > 4. Konferenz Frankfurt 22.10.2025 > PowerPoint-Präsentation: Nadine Jacobi).

Zweites Inputreferat von Manuel Heinemann «Ist doch Privatsache!- Auswirkung von externer Gewalt auf Unternehmen»

Manuel Heinemann, Kriminologe und Polizeiwissenschaftler, befasst sich in seiner Arbeit mit zielgerichteter Gewalt, darunter Amoklagen, Stalking, Radikalisierung und andere Formen schwerwiegender Gewaltphänomene. In seinem Vortrag thematisierte er die Auswirkungen privater Gewaltprobleme auf Unternehmen und zeigt, warum diese Themen keineswegs als reine Privatsache betrachtet werden sollten.

Gewalt als gesamtgesellschaftliches Phänomen

Heinemann machte deutlich, dass gesellschaftlich tabuisierte Gewalt ein grundlegendes menschliches Verhalten darstellen kann. Anhand eines kurzen interaktiven Experiments zeigte er, dass «Gewalt eine Fähigkeit des Menschen ist, welche nicht erlernt wird, sondern von Geburt an da ist». Aus seiner Sicht ist Gewalt kein Randphänomen „der anderen“, sondern betrifft Menschen in allen Lebensbereichen. Entsprechend spiegeln Unternehmen diese Realität wider.

Relevanz für Unternehmen

Das Verhalten einer fixierten oder psychisch belasteten Person kann Fehlverhalten, Leistungsabfall, Störungen des Betriebsfriedens, Sicherheitsrisiken oder sogar Gefährdung anderer Mitarbeitender verursachen. Damit berührt es zentrale Compliance-Bereiche wie Arbeitssicherheit und Fürsorgepflicht, Schutz vor Belästigung, Stalking im Unternehmen, Prävention von Eskalationen oder Gewaltrisiken, Mitarbeiterführung, Richtlinien, Meldesysteme, Umgang mit Auffälligkeiten und Risiken im Betrieb.

Heinemann erläutert, dass Unternehmen immer wieder mit privaten Problemlagen ihrer Mitarbeitenden konfrontiert werden, beispielsweise Stalking, häusliche Gewalt, Fixierungsverhalten, Radikalisierung, drohende oder zielgerichtete Gewalt. Diese Situationen können Unternehmen auf drei Ebenen massiv betreffen:

1. Sicherheitsrisiken: Etwa durch externe Täter, die die betroffene Person am Arbeitsplatz aufsuchen.
2. Wirtschaftliche Belastungen: Etwa durch Fehlzeiten, Leistungsabfall, Fehleranfälligkeit.
3. Kulturelle und psychologische Konsequenzen: Etwa Verunsicherung anderer Mitarbeitender.

Anhand einer Stalking-Prävalenz von geschätzt 7 bis 19 Prozent zeigt er auf, wie häufig entsprechende Fälle auftreten und wie oft die Auswirkungen direkt in Betrieben sichtbar werden.

Beispiele aus der Praxis

Heinemann schilderte verschiedene Fallkonstellationen aus seiner Arbeit im Bedrohungsmanagement, darunter Stalking innerhalb eines Unternehmens, also Täterinnen und Täter sowie Betroffene sind Arbeitskolleginnen oder -Kollegen, externe Stalker, die Mitarbeitende am Arbeitsplatz aufsuchen oder extreme Fixierungen, bei denen Personen über Monate oder Jahre hinweg ausschliesslich auf eine andere Person fokussiert sind.

Er beschrieb einen Fall, in dem ein Mann sieben Jahre lang ein extrem ausgeprägtes Fixierungsverhalten zeigte. Solche Situationen beeinträchtigen die Arbeitsfähigkeit gravierend, führen zu Fehlern, sinkender Produktivität und stellen oft verdeckte Sicherheitsrisiken dar.

Herausforderungen im Unternehmensalltag

Heinemann berichtete, dass Unternehmen häufig Hemmungen haben, private Probleme der Mitarbeitenden als organisationales Thema anzuerkennen. Er begegne regelmässig Aussagen wie „das ist Privatsache“. Dabei könne gerade häusliche Gewalt rasch zu einem Risiko für die gesamte Belegschaft werden, wie wenn ein gewalttätiger Ex-Partner die betroffene Person am Arbeitsplatz sucht, da dieser öffentlich zugänglich bleibt. Zugleich wies er darauf hin, dass bestehende Unterstützungsangebote (zum Beispiel Sozialberatung) oft isoliert sind und entscheidende Schnittstellen fehlen.

Diskussion und Ausblick

Im Austausch mit dem Publikum diskutierte Heinemann Fragen zur Erkennung von Fixierungsverhalten, zum Umgang mit emotional belasteten Mitarbeitenden sowie zu Möglichkeiten therapeutischer oder organisatorischer Interventionen.

Der Vortrag zeigt damit auf, dass Compliance nicht nur Regeln und Gesetze umfasst, sondern auch die präventive Verantwortung des Unternehmens, Risiken zu erkennen und angemessen darauf zu reagieren.

Paneldiskussion «Compliance im Wandel: Zwischen Verantwortung, Kultur & Kontrolle» mit Dr. Sophia Habbe, Patrick Knittel und Dr. Bárbara Lessa, moderiert von Prof. Dr. Heribert Hirte

Moderator Prof. Dr. Heribert Hirte startete die Diskussion mit Patrick Knittel, Ombudsperson Hinweisgeberschutz und Datenschutzbeauftragter. Dabei erläuterte Knittel, dass externe Hinweisgeberstellen oft als persönlicher und niedrigschwelliger wahrgenommen werden als interne Anlaufstellen. Dies liege vor allem daran, dass externe Stellen auf Augenhöhe kommunizieren und weniger Hemmschwellen bestehen als beim Kontakt mit internen Juristen oder Anwaltskanzleien.

Ein weiterer Schwerpunkt lag auf den Kosten für Hinweisgebersysteme. Patrick Knittel wies darauf hin, dass der Markt sehr unterschiedliche Preisstrukturen aufweist: Während einige Anbieter mit sehr niedrigen Einstiegspreisen werben, steigen die Kosten bei tatsächlicher Fallbearbeitung teils erheblich an. Gleichzeitig gibt es Komplettlösungen für Unternehmen ab 50 Mitarbeitenden, die bereits unter 1'000 Euro pro Jahr verfügbar sind. Diese Zahlen bieten Orientierung für die Diskussion und für Unternehmen, die ein System einführen müssen.

Prof. Dr. Heribert Hirte leitete zum Gespräch zu Dr. Bárbara Lessa über. Sie zog einen internationalen Vergleich zwischen der Rechtssysteme in Deutschland und Brasilien. Dabei berichtete sie aus ihrer Tätigkeit in einer brasilianischen Regionalregierung. Seit 2013 verfügt Brasilien über ein neues Antikorruptionsgesetz, das ein umfassendes System der Unternehmenshaftung bei Korruptions- und Betrugsfällen etabliert. Zentral sei, dass Sanktionen in Brasilien als administrative Massnahmen durch Behörden verhängt werden. Die Höhe der Geldbussen orientiert sich am Unternehmensumsatz. Zudem werde stets bewertet, ob ein wirksames Compliance-Programm besteht: Ein solches kann die Busse um bis zu fünf Prozent senken, weitergehende Kooperation ermöglicht eine Reduktion um bis zu zwei Drittel. Grosse Korruptionsskandale hätten erheblichen Druck erzeugt, Compliance-Strukturen zu stärken. Das brasilianische System setze deshalb klar auf Anreize zur Implementierung wirksamer Programme.

Dr. Bárbara Lessa verglich, dass Anreizmechanismen in Brasilien deutlicher ausgeprägt sind als in Deutschland. Dort sei zwar ein ähnliches Modell diskutiert worden, das höhere Bussgelder und stärkere Belohnungen für Compliance-Programme vorsieht, jedoch teilweise kritisiert wurde, weil es zu finanziellen Verflechtungen zwischen Staat und beratenden Kanzleien führen könnte.

Der Moderator und Dr. Bárbara Lessa gingen anschliessend der Frage nach, ob finanzielle Anreize bei der Verfolgung von Korruptionsfällen eine Rolle spielen, sowohl für Unternehmen als auch für staatliche Stellen. In Brasilien habe es hierzu intensive Diskussionen gegeben, da das Antikorruptionsgesetz viele Fälle mit hohen Bussgeldern ausgelöst habe und der Markt für Kanzleien wie Behörden gewachsen sei. Dadurch sei der Eindruck entstanden, beide Seiten hätten ein finanzielles Interesse an Sanktionen. Als Reaktion bemühe man sich heute um mehr Transparenz bei der Berechnung von Geldbussen. Diese bestehen aus einer eigentlichen Sanktion und einem oft deutlich höheren Anteil zur Schadenskompensation.

Kritisch diskutiert wurde zudem, wohin die Gelder fliessen. Obwohl sie der Kompensation dienen, würden sie häufig dem Staatshaushalt zugeführt statt direkt den geschädigten Einrichtungen oder dem Volk. Dies verstärkte die Diskussion, ob der Staat finanziell von Korruptionsfällen profitiere und ob das System ausreichende Anreize für Prävention statt Sanktionierung schafft.

Zum Schluss widmeten sich Dr. Sophia Habbe und Prof. Dr. Heribert Hirte der Rolle des Aufsichtsrats im Compliance-System. Dr. Sophia Habbe stellte fest, dass sich die Diskussion hierzu in den letzten zehn Jahren deutlich weiterentwickelt hat. Während früher unklar war, welche Befugnisse der Aufsichtsrat bei Untersuchungen, etwa gegenüber Mitarbeitenden oder Vorstandsmitgliedern, besitzt, besteht heute ein klareres Verständnis. Zentral ist die Abgrenzung der Verantwortlichkeiten: Die operative Compliance- und Risikoverantwortung liegt beim Vorstand, während der Aufsichtsrat eine überwachende und beratende Funktion ausübt. Da er ein Nebenamt wahrnimmt und nicht operativ eingebunden ist, müsse sorgfältig geprüft werden, wie weit seine praktische Rolle reicht.

Besonders umstritten ist die Frage, ob der Aufsichtsrat selbst als Meldestelle fungieren kann. Organisatorisch sei dies schwierig, da Meldestellen oft nicht beurteilen können, welche Hinweise für den Aufsichtsrat relevant sind, insbesondere bei komplexen Sachverhalten mit möglichem

Organisationsverschulden. Dr. Sophia Habbe stellte die Bedeutung klarer, verständlicher Prozesse zur Weiterleitung relevanter Meldungen fest. Obwohl die Rechtslage weitgehend geklärt sei, hapere es in der Praxis häufig an der Umsetzung. Zudem sei der Aufsichtsrat kein homogenes Gremium, unterschiedliche Interessen können die Zusammenarbeit erschweren. In sensiblen Fällen würde daher oft nur der Vorsitzende oder der Prüfungsausschuss eingebunden, um Vertraulichkeit zu wahren.

Habbe erläuterte die Folgen der Einbindung des Aufsichtsrats in Compliance- und Whistleblowing-Prozesse. Entscheidend sei, welche Pflichten den Aufsichtsrat treffen, sobald Hinweise auf Fehlverhalten bekannt werden, vor allem bei Verdachtsmomenten gegen Vorstandsmitglieder. In der Praxis werde häufig zunächst nur der Vorsitzende informiert. Nach ihrer Erfahrung braucht es keine zusätzlichen Strukturen wie eine eigene Aufsichtsratshotline. Bewährt habe sich vielmehr ein abgestimmtes Budget, mit dem externe Kanzleien bei Bedarf mandatiert werden können. Der Umfang der Einbindung richte sich nach der Schwere des Vorwurfs: Bei Hinweisen gegen ein einzelnes Vorstandsmitglied übernimmt meist der übrige Vorstand die Aufklärung, während der Aufsichtsrat plausibilisiert. Bei schwerwiegenden oder mehrere Mitglieder betreffenden Vorwürfen wird der Aufsichtsrat intensiver eingebunden.

Dr. Sophia Habbe warnte vor zusätzlicher Bürokratie. Angesichts steigender regulatorischer Anforderungen sei die Rolle des Aufsichtsrats bereits komplex. Wichtig sei eine funktionierende und unabhängige Berichts- und Informationskette, wie etwa über Compliance, Audit oder den General Counsel, damit der Aufsichtsrat die wesentlichen Entwicklungen versteht und angemessen reagieren kann.

Auf die Frage nach dem Eingang von Hinweisen erklärte sie, dass diese meist über den General Counsel an den Aufsichtsrat gelangen, da dieser die rechtliche Relevanz beurteilen könne. Viele Hinweise seien Zufallsfunde oder beträfen Kultur- und Organisationsfragen.

Interview mit Paul Welter «Compliance automatisieren mit KI»

Der per Videokonferenz zugeschaltete Referent Paul Welter, Programmierer und Rechtsanwalt, gab einen Einblick in die Schnittstelle zwischen Recht und Künstlicher Intelligenz (KI). Er erläuterte, dass er sich seit seiner Ausbildung mit der Frage beschäftigt, wie juristische Arbeit automatisiert werden kann. Aktuell arbeitet er an KI-Lösungen für grosse Unternehmen und entwickelt Systeme zur effizienteren juristischen Informationsverarbeitung.

Herausforderungen in heutigen Compliance-Abteilungen

Paul Welter stellte aus technischer Perspektive zwei zentrale Probleme fest. Zum einen die Informationsasymmetrie: Zwischen Business und Compliance bestehen Wissens- und Entscheidungsunterschiede. Mitarbeitende im operativen Bereich kennen die Fakten eines Sachverhalts, jedoch häufig nicht die relevanten Regeln. Compliance hingegen kennt die Regeln, muss aber den Sachverhalt mühsam in Erfahrung bringen. Dies führt zu zeitintensivem Austausch und Verzögerungen. Zum anderen erfolgen viele Compliance-Entscheidungen über einfache Rückfragen, E-Mail-Pingpong und manuelle Prüfungsschritte. Dadurch entstehen Engpässe, welche Compliance zu einem „Bottleneck“ werden lassen.

Einsatz von KI: Chancen und Grenzen

Paul Welter erklärte, dass KI juristische Subsumtionsprozesse, also die Anwendung von Regeln auf konkrete Sachverhalte, erstmals technisch zuverlässig unterstützen kann. Dies ermögliche automatisierte Erstbewertungen, etwa über Chatbots, die einfache Compliance-Fragen schnell beantworten können. Gleichzeitig verwies er auf die Notwendigkeit klarer Rahmenbedingungen:

Transparenz und Nachvollziehbarkeit: Reine Deep-Learning-Modelle seien für Compliance ungeeignet, da sie keine transparenten Begründungen liefern. KI müsse deshalb in kontrollierbare Workflows eingebettet werden.

Kontrolle durch „Human in the Loop": Komplexe, psychologisch geprägte oder risikoreiche Fälle dürften nicht automatisiert werden. Systeme müssten solche Themen automatisch eskalieren.

Datenschutz und Vertraulichkeit: In Bezug auf sensible Eingaben, etwa potenziell belastende Sachverhalte, erklärte Welter, dass technische Schutzmechanismen notwendig seien wie Filter, die heikle Fälle sofort an externe oder interne Meldestellen weiterleiten. Es braucht auch Hosting-Modelle, die Daten im Unternehmen oder bei vertraglich streng gebundenen Dienstleistern halten sowie klare Vorgaben, ob und wie Konversationen gespeichert oder sofort gelöscht werden. Beides sei konfigurierbar und letztlich eine Frage der Unternehmenskultur.

Ein Blick in die Zukunft

Für die kommenden Jahre erwartet Paul Welter:

- Eine deutliche Automatisierung einfacher juristischer Routineprozesse.
- KI-Systeme, die ganze Workflows steuern statt nur Einzelschritte.
- Eine Entwicklung hin zu Compliance-Abteilungen, die vermehrt überwachend und steuernd agieren, während KI Standardfälle autonom abarbeitet.

Paneldiskussion: «Corporate Governance und Compliance in der Praxis» mit Julia Arbery, LL.M., Prof. Dr. Julia Redenius-Hövermann und Dr. Rolf Raum, moderiert von Dr. Martin Weimann

Im abschliessenden Panel reflektierten die drei Panelisten und der Moderator die Beiträge der gesamten Konferenz. Sie griffen die Inhalte der Vorträge, Interviews und vorangegangenen Diskussionen noch einmal auf und ordneten diese im Gesamtkontext ein und brachten ihre eigene Perspektive mit ein.

Hinweisgeberschutz

In Bezug auf das Einstiegsreferat nahm Panelistin Julia Arbery die Bedeutung von Vertrauen im Hinweisgebersystem nochmals auf. Sie wies jedoch darauf hin, dass insbesondere jüngere Mitarbeitende zunehmend lieber anonyme digitale Hinweise abgeben, statt direkt mit einer Person zu sprechen. Sie erklärte, dass Anonymität nach amerikanischem Compliance-Verständnis ein wichtiger Faktor sei, um möglichst viele Hinweise zu erhalten. Durch den Schutz der Anonymität seien Hinweisgeberinnen und Hinweisgeber eher bereit, Informationen zu teilen, auch wenn sie sich später eventuell zu erkennen geben würden. Julia Arbery hob hervor, dass Hinweise oft zunächst informell im privaten Umfeld diskutiert werden – etwa zu Hause, mit Freunden oder Kolleginnen sowie Kollegen – bevor sie in das Unternehmen gelangen. Für die Organisation sei es entscheidend, den Hinweisgebern Sicherheit innerhalb der Organisation zu bieten, damit die Informationen intern bearbeitet werden können, bevor sie an externe Stellen wie die Presse oder Staatsanwaltschaft gelangen.

Dr. Rolf Raum sprach über seine Erfahrungen mit Anonymität in Strafverfahren und stellte klar, dass es keine anonymen Zeugen gibt. Zwar existieren nicht-öffentliche Hinweise, etwa von verdeckt arbeitenden Polizeibeamtinnen und -beamten, diese werden jedoch sehr restriktiv behandelt, da die Richterin oder der Richter grundsätzlich auf persönlich vernommenen Aussagen vertraut. Hinweise vom Hörensagen können zwar unter bestimmten Umständen ausreichen, sind aber oft problematisch, besonders wenn es um die Identifizierung von Hinweisgeberinnen und Hinweisgeber geht. Er erläuterte, dass bei detaillierten Hinweisen oft Rückschlüsse auf die Identität des Hinweisgebenden möglich seien. Moderne Technologien wie digitale Bild- oder Geodaten könnten zudem die Anonymität gefährden.

Verstösse und Bussgelder

Vor dem Hintergrund des Inputs von Dr. Bárbara Lessa erläuterte Dr. Rolf Raum die Bedeutung von Compliance-Systemen im deutschen Recht, insbesondere im Kartellrecht. Er hob hervor, dass sowohl bestehende als auch nachträglich implementierte Compliance-Programme mittlerweile bei der Bussgeldbemessung berücksichtigt werden, was positiv gelöst sei. Im Gegensatz dazu habe das frühere Verbandssanktionengesetz mit umfangreicher Bürokratie und Monitoring nicht überzeugt.

Entscheidend sei die konkrete Umsetzung im Unternehmen: Ein rudimentäres Compliance-System sei nur symbolisch wirksam, während schwerwiegende Verstösse, etwa durch den Vorstand, zu klaren Konsequenzen wie dem Wegfall von Boni führen. Auch bei nachträglich eingeführten Programmen müsse die Justiz prüfen, ob sie wirksam sind, was die Gerichte erheblich belaste und Widersprüche erzeugen könne. Raum sagte, dass ein gut ausgeprägtes Compliance-System Unternehmen vor Haftung schützen kann, auch wenn einzelne Mitarbeiter Fehlverhalten zeigen. Die Verantwortung eines Vorstandsmitglieds oder einzelner Mitarbeiter könne sich vom Unternehmen abgrenzen, wobei Bussgelder auch bei Verstössen unterhalb der Vorstandsebene verhängt werden können.

Abschliessend wies Raum auf die zentrale Rolle der Abschreckung hin: Hohe Bussgelder erzeugten Angst, die als wesentlicher Triebfaktor für Compliance diene. Eine Reduzierung der Bussgelder führe automatisch zu geringerer Compliance-Motivation, da kalkulierbare Strafen die präventive Wirkung mindern. Raum unterstrich die Notwendigkeit von Rechtssicherheit, betonte aber, dass ein gewisser Unsicherheitsfaktor im Bussgeldwesen auch zum Wesen von Strafen gehöre.

Aufsichtsrat

Julia Redenius-Hövermann brachte ihre Perspektive zum Thema über die Rolle des Aufsichtsrats im Compliance-System ein und fragte, wo Compliance angesiedelt sein sollte. Es wurde klargestellt, dass Compliance primär unter dem Vorstand angesiedelt ist und der Aufsichtsrat dessen Überwachung und Beratung übernimmt. Gleichzeitig besteht für den Aufsichtsrat die Möglichkeit, direkt auf Compliance-Berichte zuzugreifen, ohne die dualistische Struktur des deutschen Systems zu untergraben.

Auch Julia Arbery äusserte sich zum Input von Dr. Sophia Habbe zu den Aufsichtsräten: Wie Organisationen eine Kultur fördern können, die rechtskonformes Verhalten unterstützt und zugleich Anreize schafft. Dabei wurde das Spannungsfeld zwischen der Notwendigkeit von Konsequenzen bei Fehlverhalten und der Förderung von Compliance hervorgehoben. Als Beispiel wurde das amerikanische Prinzip „skin in the game“ genannt: Führungskräfte und Vorstände sollten persönlich von rechtskonformem Handeln profitieren, etwa über bonusrelevante Anreize, um ein wirksames Compliance-System zu unterstützen. Gleichzeitig hoben die Diskutierenden hervor, dass auch die Furcht vor Sanktionen ein wesentlicher Bestandteil wirksamer Compliance bleibt.

Künstliche Intelligenz

Julia Redenius-Hövermann sprach über den Einsatz von KI im Compliance- und Entscheidungsbereich. Sie stellte fest, dass KI derzeit vor allem als Hilfsmittel zur Entscheidungsunterstützung genutzt werden kann, etwa für Recherchen oder die Aufbereitung von Lösungsansätzen. Eine Verlagerung der Entscheidungsverantwortung von Menschen auf KI sei rechtlich nicht zulässig: Die letztendliche Verantwortung verbleibt beim Vorstand oder der verantwortlichen Person. KI kann unterstützen, die Entscheidung jedoch nicht ersetzen.

Julia Arbery thematisierte die Chancen und Herausforderungen von KI im Unternehmenskontext. Sie sieht den Einsatz insbesondere für wiederkehrende Prozesse mit geringem Risiko als sinnvoll, zeigte jedoch die Schwierigkeiten bei Entscheidungen auf, die keine klare Wiederholbarkeit oder Erklärbarkeit

haben. Die Verantwortung für die Entscheidung bleibt kritisch, und derzeit fehlen noch praktische Erfahrungswerte, um KI zuverlässig einzusetzen.

Zum Schluss fasste Rolf Raum zusammen, dass die Verantwortung für den Einsatz von KI stets bei der Person oder Organisation liegt, die sie nutzt. Eine Haftungsvermeidung durch die blosse Nutzung von KI sei nicht möglich.

Drittes Inputreferat von Dr. Mirjam Weisse «EU Whistleblowing Richtlinie (EU 2019/1937) vs. Corporate Governance?»

Dr. Mirjam Weisse griff in ihrem Vortrag das Thema der praktischen Umsetzung der EU-Whistleblowing-Richtlinie in multinationalen Konzernen und die damit verbundenen Herausforderungen aus Sicht der Corporate Governance. Sie wählte bewusst einen provokanten Titel mit Fragezeichen. Ein Hinweis darauf, dass die Vorgaben der Richtlinie mit in der strukturellen Realität multinationaler Unternehmen oft schwer zu vereinbaren sind.

Spannungsfeld EU-Richtlinie und Unternehmensrealität / Vorgaben der Corporate Governance

Weisse erklärte, dass multinationale Unternehmen nicht nur ein nationales Recht, sondern die Vorschriften zahlreicher Länder gleichzeitig berücksichtigen müssen. Dies führe zu hoher Komplexität und erschwere den Überblick erheblich. Besonders problematisch seien die Anforderungen hinsichtlich dezentraler Hinweisgebersysteme, die laut Richtlinie für jede Einheit mit nur 250 Mitarbeitenden (einer kleinen Unternehmensgrösse) gelten. In der Praxis zeige sich jedoch, dass Hinweisgeber am meisten von einem zentral professionell betriebenen System profitieren, während lokale Kanäle Potential für Risiken und Ineffizienzen bergen.

Umsetzungspraxis und Herausforderungen

Unternehmen versuchten aktuell, etwa 80 Prozent der Vorschriften konsequent umzusetzen. Die restlichen 20 Prozent würden pragmatisch gehandhabt, wenn sie widersprüchlich oder so unpraktikabel seien, dass das Ziel der Richtlinie verfehlt werde.

Weisse warnte, dass Mitarbeiter, die Meldungen abgeben möchten, sich in dem bestehenden Regelungsdickicht theoretisch selbst Haftungs- oder Ordnungswidrigkeitenrisiken aussetzen könnten, weil die Bestimmungen soweit und gleichzeitig so unklar bzw. weich formuliert sind, dass der Hinweisgeber kaum überblicken könne, wann eine Meldung den Schutzbereich eröffnet und welche Betroffenenrechte oder Geheimhaltungsvorschriften einer Meldung entgegenstehen könnten.

Internationale Unterschiede und Rechtsunsicherheit

Ein weiterer zentraler Punkt des Vortrags war die internationale Dimension: Die Definition der meldefähigen Tatbestände und dazugehörende Rechtsauffassungen variiere stark zwischen den EU-Ländern und zusätzlich weiteren Nicht-EU-Ländern, die ebenfalls Regelungen zum Schutz von Hinweisgebern vorsehen. Dies erschwere nicht nur die Bearbeitung der Hinweisvorgänge an sich, sondern auch eine stringente Berichterstattung gegenüber der Geschäftsleitung, als Teil des Corporate Governance Pflichtenkatalogs. Dies lasse sich an verschiedenen Beispielen, wie etwa nationalen Informationssicherheitsgesetzen oder auch an Straftatbeständen im Wirtschaftsstrafrecht eindrucksvoll durchspielen.

Lösungsansatz: Zentrale Investigation-Abteilungen

Dr. Mirjam Weisse präsentierte als praktikable Lösung die Einrichtung zentraler Investigation-Abteilungen, in denen Meldungen gesammelt und professionell bearbeitet werden. Diese sollten durch lokale Kontaktpunkte (ggf. ausserhalb der lokalen Einheit durch Dritte, wie etwa Ombudspersonen) ergänzt

werden, welche die Pflicht zur lokalen Meldeoption umsetzen, die aber gezielt und soweit erforderlich um personenbezogene Daten (oder den Identitätsschutz des Hinweisgebers gefährdende Informationen) bereinigt auf das zentrale System geleitet werden, um Professionalität, Vertraulichkeit und Effizienz zu gewährleisten. Wichtig sei es, die immanenten Vorteile für die Hinweisgeber zu beachten: Eine von der lokalen Geschäftsleitung unabhängige, zentrale oder zentral koordinierte Aufarbeitung ermögliche es deutlich besser, die Identität des Hinweisgebers vertraulich zu halten und Repressalien zu verhindern und damit das erklärte Ziel der Richtlinie zu verwirklichen. In großen internationalen Konzernen habe sich dieses Vorgehen über Jahre bewährt, ohne dass die rein lokale Bearbeitung lokaler Meldungen notwendig gewesen wäre.

Fazit

Abschliessend zog Weisse das Fazit, dass die EU-Richtlinie Unternehmen vor erhebliche Herausforderungen stelle. Zentrale Systeme böten die beste Möglichkeit, Hinweisgeber zu schützen, Prozesse effizient zu gestalten und Risiken zu minimieren. Dezentrale Ansätze hingegen seien häufig ineffizient und risikobehaftet, wenn keine gezielte Koordination und Steuerung stattfände.

Abschluss der Konferenz

Prof. Dr. Patrick Krauskopf dankte allen Speakerinnen und Speaker, Teilnehmerinnen und Teilnehmer, den Moderatoren sowie dem Institutsrat Prof. Christian Strenger, der seine Räumlichkeiten der Frankfurt School zur Verfügung stellte.

Die 4. Konferenz zu Compliance, Whistleblowing und Corporate Governance an der Frankfurt School bot den Teilnehmenden einen praxisnahen Einblick in die aktuellen Herausforderungen und Entwicklungen auf nationaler und internationaler Ebene. Die Vorträge und Paneldiskussionen zeigten deutlich, dass Compliance nicht nur eine juristische Pflicht, sondern ein komplexes Zusammenspiel aus rechtlichen Anforderungen, organisatorischer Umsetzung und Unternehmenskultur ist.

Die 7. ICW-Konferenz in Frankfurt ist für den 21. Oktober 2026 geplant.

Autorin: Hannah Wenger