Compliance

Die Zeitschrift für Compliance-Verantwortliche

September 2024

SCHWERPUNKT FINANCE

Inhalt

© IMAGO / Metodi Popow

Aufmacher

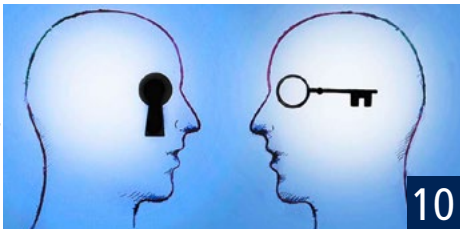
Streit um Gesetz zur Bekämpfung von Finanzkriminalität
Am 26. Juni 2024 hatte der Finanzausschuss den Gesetzentwurf der Bundesregierung (20/9648) zur Verbesserung der Bekämpfung von Finanzkriminalität verabschiedet. Den Bundestag passierte das neue Gesetz jedoch anschließend nicht. Vor allem zum Thema Kompetenzverteilung bzgl. einer neuen Geldwäschebehörde entzündet sich derzeit Streit.

Recht

© IMAGO / Zoonar

ESMA veröffentlicht Leitlinien zu Fondsnamen
Die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) hat Leitlinien für Fondsnamen veröffentlicht. Sie sollen klären, unter welchen Bedingungen ein Fonds im Namen Wörter wie Umwelt, Soziales, gute Unternehmensführung oder andere nachhaltigkeitsbezogene Begriffe verwenden kann.

Kolumne



© IMAGO / Ikon Images

Kolumne: Spielräume erkennen
In den vorherigen Ausgaben hat unser Kolumnist Markus Jüttner den Begriff des „Systems" für die Compliance näher beleuchtet, insbesondere was ein Compliance-System von einem Compliance-Haufen unterscheidet und wann man von einem integrierten Compliance-Management-System (CMS) sprechen kann. Ein bedeutsamer Blickwinkel wurde aber noch nicht betrachtet, nämlich der Kontext.

Praxis

© IMAGO / Westend61

Die Implementierung eines KI Governance Frameworks
Es ist inzwischen keine Frage mehr, ob KI in einem Unternehmen eingesetzt wird, sondern vielmehr in welchem Umfang und welche Bereiche und Prozesse betroffen sind. Der Einsatz von KI bringt allerdings auch regulatorische und ethische Risiken mit sich, denen sich Unternehmen stellen müssen.

Veranstaltungen

11.-13.09.2024 | Düsseldorf oder Online | **Datenschutzkonferenz**

20.09.2024 | Frankfurt am Main oder Online | **10. Deutscher Glücksspielrechtstag**

01.10.2024 | Frankfurt am Main | **2. Jahrestagung Geldwäsche & Recht**

10.10.2024 | Frankfurt am Main | **Datenschutz bei internen Ermittlungen**

24.10.2024 | München | **1. Deutscher Beschäftigtendatenschutztag**

15.10.2024 | Bonn | **Sorgfaltspflichten entlang von Lieferketten**

Streit um Gesetz zur Bekämpfung von Finanzkriminalität

Am 26. Juni 2024 hatte der Finanzausschuss den Gesetzentwurf der Bundesregierung (20/9648) zur Verbesserung der Bekämpfung von Finanzkriminalität (Finanzkriminalitätsbekämpfungsgesetz) mit den Stimmen der Koalitionsfraktionen von SPD, Bündnis 90/Die Grünen und FDP gegen die Stimmen der CDU/CSU- und der AfD-Fraktion sowie der Gruppe Die Linke verabschiedet. Den Bundestag passierte das neue Gesetz jedoch anschließend nicht – trotz der Einigkeit der Regierungsfraktionen im Ausschuss. Vor allem die Kompetenzverteilung im Zusammenhang mit der geplanten neuen Geldwäschebehörde ist ein Thema, an dem sich derzeit Streit entzündet.

© IMAGO / Metodi Popow

Die Kritik an der neuen Geldwäsche-Behörde ist nicht neu: Demonstranten im Oktober 2023.

Aus den Parlamentsnachrichten zur Finanzausschusssitzung ließ sich zwar entnehmen, dass die Opposition nicht mit dem Gesetzentwurf d'accord ging, dass es aber letztlich Mitglieder der Regierungskoalition selbst sein würden, die auf der Bremse stehen, danach sah es zunächst nicht aus: Kurz vor der Sitzung des Finanzausschusses hatten die Ampel-Fraktionen noch sechs Änderungsanträge eingebracht, die sogar auf teilweise Zustimmung der Unionsfraktion stießen. An der grundlegenden Ablehnung der Opposition konnte das zwar nichts ändern, doch das Gesetz passierte den Finanzausschuss dank der Stimmen der Ampelfraktionen. Die Kritik der Opposition blieb außen vor: Die Unionsfraktion warnte vor Parallelstrukturen durch verschiedene Behörden. Dieser Umstand erschwere es auch, ausreichend qualifiziertes Personal zu gewinnen, wobei die Gefahr bestehe, dass die verschiedenen Behörden sich gegenseitig Mitarbeiter abwerben. Die AfD-Fraktion bemängelte, dass es nicht eine zentrale Behörde gebe, dies auch mit Blick auf die Kompetenzen der Bundesländer. Die Gruppe Die Linke konstatierte, der Gesetzentwurf sei hinter den Referentenentwurf zurückgefallen. Die beteiligten Behörden würden auch künftig getrennt voneinander agieren.

Die Ampel-Fraktionen hielten dagegen und zogen während der Beratungen zum Gesetzesentwurf im Finanzausschuss an einem Strang. Sowohl FDP als auch Grüne wiesen darauf hin, die Ampel-Koalition habe die Kritik der internationalen Standardsetzerin im Bereich Geldwäsche, der FATF, an Deutschland aufgegriffen und orientiere sich mit ihrem Gesetzentwurf an den Empfehlungen der FATF. Aus der FDP hieß es, künftig werde wie international üblich im Kampf gegen Geldwäsche ein „Follow-the-Money-Ansatz" verfolgt. Es gehe um dicke Fische und Sanktionsbrecher.

Diese Einmütigkeit konnte aber im weiteren Verlauf des Gesetzgebungsverfahrens offenbar nicht eingehalten werden. Inzwischen wirft die FDP der Grünen-Fraktion eine Blockadehaltung bei der Verabschiedung des Gesetzes vor. Gleichzeitig wird über die Medien die Vermutung verbreitet, das Gesetz werde von den Grünen mit den Verhandlungen über eine Neuregelung der Kindergrundsicherung politisch verknüpft. Denn auch hierüber streitet die Regierungskoalition – namentlich FDP und Grüne – seit längerem.

Tatsächlich hatten die Grünen eine Verabschiedung des Gesetzes zur Bekämpfung von Finanzkriminalität in der letzten Parlamentswoche vor der Sommerpause verhindert und darauf hingewiesen, dass zunächst ein Gesetzentwurf zur Bekämpfung von Vermögensverschleierung auf den Weg gebracht werden müsse. Die Einrichtung einer neuen Behörde, die im Finanzkriminalitätsbekämpfungsgesetz vorgesehen ist, mache keinen Sinn, wenn diese nicht entsprechende Befugnisse habe.

Auf der Plattform X äußerte sich Bundesfinanzminister Christian Lindner Anfang Juli hierzu drastisch gegenüber dem Koalitionspartner: „Es ist kein guter Grund, dass die Grünen noch auf das Instrument der Vermögensermittlung warten wollen. Denn es geht Zeit verloren. Mafia und Clans lachen sich kaputt."

Ob und wann das Gesetz zur Bekämpfung der Finanzkriminalität nun beschlossen wird, ist aktuell weiter unklar. Immerhin ist die neue Geldwäschebehörde, das Bundesamt zur Bekämpfung von Finanzkriminalität (BBF), bereits im Haushalt 2025 veranschlagt. Für diese im Rahmen des Finanzkriminalitätsbekämpfungsgesetzes zu schaffende neue Behörde sind für 2025 Gesamtausgaben von 179 Mio. EUR vorgesehen. Die Zahl der Stellen im neuen Bundesamt soll auf 983 ansteigen.

Überhaupt kein gutes Haar lässt die Gewerkschaft der Polizei, Bezirksgruppe Zoll, in einer Pressemeldung an der neuen Behörde: Die Ampel gehe nach ihren Aussagen irrigerweise davon aus, dass ein paar wenige zusätzliche Beamte in einem neuen Ermittlungszentrum Geldwäsche in einer ganz neuen Behörde das Problem bei der Bekämpfung von Finanzkriminalität lösen könnten. „Als ob das Heil der Bekämpfung der Finanzkriminalität in einem neuen und zentralen ‚Hort der Kompetenz' läge, obwohl die strafrechtliche Geldwäschebekämpfung ohnehin grundsätzlich Aufgabe der Länder ist und der Bund nur in ganz ausgewählten Fällen beim BKA und beim Zoll eine Zuständigkeit hat." Stattdessen könnte der Bund „einerseits seine erfahrenen und in die Sicherheitsarchitektur integrierten Ermittlungsdienste beim BKA und im Zoll in den bestehenden Strukturen deutlich stärken und zudem die Kontroll-, Fahndungs- und Ermittlungsdienste endlich zu einer schlagkräftigen Finanzpolizei ausbauen". Finanzminister Lindner führe mit dem „Extra-Amt" indes lieber das Theaterstück „Viel Lärm um Nichts" für die FATF auf.

chk

Hybrid-Veranstaltung: Teilnahme vor Ort sowie Online möglich!

Datenschutzkonferenz 2024

Praxis | Recht | Innovation

11. - 13. September 2024 | Hotel Kö59 Düsseldorf

Es erwarten Sie u. a. diese Themen:

- Scoring zur Steuerung von Kundenbetreuung und Unternehmensprozessen
- Update Beschäftigtendatenschutz
- Betroffenenrechte aus verschiedenen Perspektiven
- Praxisvortrag: Wie bekomme ich Mitarbeiter dazu den Datenschutz zu lieben
- Verteidigung im Bußgeldverfahren
- Data Act und DSGVO: Flucht in den Personenbezug zum Schutz vor Datenzugang?
- Implementierung neuer Datenregulierung im Unternehmen
- Wer? Wie? Was? Warum? – Prüfstrategien der Aufsichtsbehörden
- Aktuelles zum Schadenersatz nach Art. 82 DSGVO
- Datenschutz-Compliance messbar machen

Freuen Sie sich auf neue Impulse durch:


Dr. Eren Basar


Kirsten Bock


Daniel Gabel


Dr. Jan-Michael Grages


Stefanie Koch


Carolin Loy


Dr. Flemming Moos


Stephan Hansen-Oest


Dr. Aileen Pasquariello


Frederick Richter


Bettina Robrecht


Maria Christina Rost


Dr. Dominik Sorber


Rebekka Weiß

Und vielen weiteren Referentinnen und Referenten.

Melden Sie sich jetzt an! **www.datenschutzkonferenz.de**

Anmeldungen & organisatorische Rückfragen an:
Herrn Jasha Baniashraf
Deutscher Fachverlag GmbH
Telefon: 069/7595-2773
Fax: 069/7595-1150
E-Mail: Jasha.Baniashraf@dfv.de

Medienpartner:
DATENSCHUTZ-BERATER
Kommunikation & Recht
Compliance Berater

ESMA veröffentlicht Leitlinien zu Fondsnamen

Die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) hat Leitlinien für Fondsnamen veröffentlicht. Die **Leitlinien** setzen sich mit der Frage auseinander, unter welchen Bedingungen ein Fonds im Namen Wörter wie Umwelt (Environment), Soziales (Social), gute Unternehmensführung (Governance) oder andere nachhaltigkeitsbezogene Begriffe verwenden kann. Damit gibt es auf diesem Feld zum ersten Mal europaweit einheitliche Vorgaben. Wie die BaFin mitteilt, wird sie die ESMA-Leitlinien in ihrer Verwaltungspraxis berücksichtigen.

Environment, Social, Governance: Fonds mit diesen Wörtern im Namen müssen bestimmte Bedingungen erfüllen.

Der Name eines Fonds vermittle einen ersten Eindruck von der Anlagestrategie und den Anlagezielen des Produkts und beeinflusse die Entscheidungen der Anleger. Die Änderung der Richtlinie über die Verwalter alternativer Investmentfonds und der Richtlinie zu Organismen für gemeinsame Anlagen in Wertpapieren beinhalte darum das Mandat an die ESMA, Leitlinien zu Fondsnamen zu entwickeln. Das erläutert die BaFin in einer Mitteilung, in der sie auch ankündigt, dass die neuen ESMA-Leitlinien die bisherige BaFin-Verwaltungspraxis zu nachhaltigen Investmentvermögen vollständig ablösen werden.

Die ESMA lege nicht nur fest, wie und in welcher Höhe der Fonds in bestimmte Vermögensgegenstände investieren muss, damit er in einer bestimmten Art und Weise bezeichnet werden darf. Sie führe darüber hinaus unterschiedliche Mindestausschlüsse ein. Diese richten sich nach der sog. Benchmark-Verordnung (EU) 2016/1011, die zwei nachhaltigkeitsbezogene Referenzwerte enthalte: Den so genannten Referenzwert für den klimabedingten Wandel (Climate Transition Benchmark (CTB)) und den Paris-abgestimmten EU-Referenzwert (Paris-Aligned Benchmark (PAB)), wobei der PAB mehr und höhere Mindestausschlüsse enthält, also „strenger" ist. Diese Ausschlüsse richteten sich zwar ausschließlich an die Administratoren von EU-Referenzwerten; die ESMA-Leitlinien machen sich aber diese Ausschlüsse zu eigen, indem sie darauf Bezug nehmen. Je nach Bezeichnung des jeweiligen Fonds gelten entweder die strengeren Mindestausschlüsse des PAB oder die weniger strengen Ausschlüsse des CTB.

chk

Data Responsibility Platform

Für jede datenrechtliche Anforderung eine Lösung

Die caralegal Data Responsibility Platform ist die Lösung für alle, die datenrechtliche Compliance mit Leichtigkeit managen wollen. Mit intuitiven Workflows und automatisierten Prozessen erfüllen Sie alle gesetzlichen Vorgaben und behalten den Überblick – von Datenschutz über Risikomanagement bis zu Audits und KI-Management. Niemand macht datenrechtliche Compliance so leicht wie caralegal.

Unsere modulare und verknüpfte Plattform beinhaltet folgende Lösungen:

Privacy Flow

Datenschutzmanagement - jetzt einfach: caralegal verbindet ExpertInnen mit Fachbereichen, automatisiert Routinetätigkeiten und gibt passgenaue Empfehlungen.

Risk Flow

Endlich zuverlässige Steuerung und Einordnung von Risiken. Sie legen die Maßnahmen fest und vereinheitlichen Arbeitsabläufe.

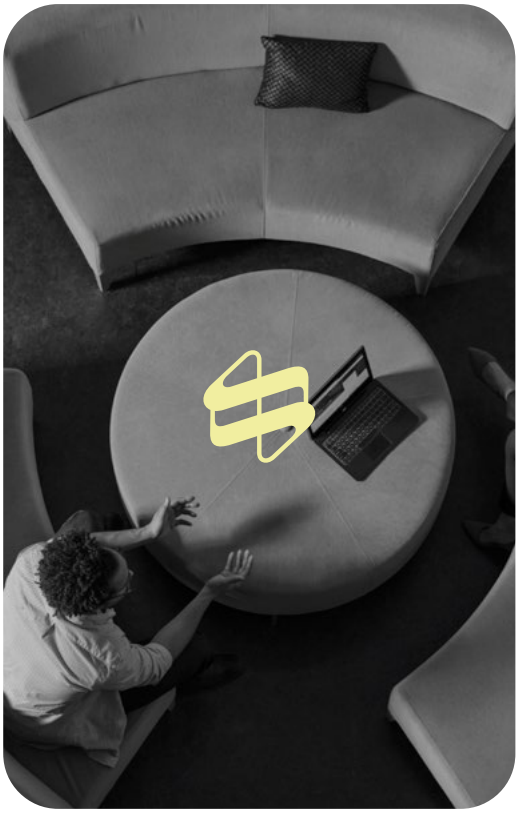
AI Flow

Identifizieren und klassifizieren Sie Ihre KI-Systeme, analysieren Modelle auf Fairness und Bias, und steuern Risiken im gesamten KI-Lebenszyklus.

Audit & Vendor Flow

Sie gestalten passgenaue Fragebögen, automatisieren administrative Tätigkeiten und skalieren Ihre Third-Party Assessments.

Jetzt die neue Leichtigkeit entdecken! →



Das erreichen Sie mit unseren Flows:

Endlich nur eine Dokumentation - mit einer verknüpften Single Source of Truth

Mehr Zeit dank Automatisierung - Compliance-Prozesse vereinheitlichen

Alle Fachbereiche machen mit, weil die „Rechts-Sprache" verständlich wird

*Wir kümmern uns um den **vollständigen Import** Ihrer bestehenden Dokumentation. Um Ihnen einen optimalen Start zu ermöglichen, übernehmen wir das als Inklusivleistung.*

DSGVO-Schadensersatz als Compliance-Risiko

Die Einhaltung gesetzlicher und damit auch datenschutzrechtlicher Vorgaben ist nicht nur aus Gründen gesetzeskonformen Handelns für Unternehmen wichtig. Auch die Inanspruchnahme durch Klagen auf (immateriellen) Schadensersatz stellt ein erhebliches Risiko dar, wie Prof. Dr. Fuhlrott erläutert.

In Sorge um ein Datenleck: Das kann schon reichen, um Schadensersatzansprüche zu begründen.

FCPA, UK Bribery Act, KWG, GWG, OWiG und der Deutsche Corporate Governance Kodex (DCGK) verpflichten zu bzw. verlangen eine verantwortungsvolle und rechtsförmige Unternehmensführung auf Basis anwendbarer Rechtsnormen und entsprechender Corporate Governance Kodizes. Bestandteil dieses Pflichtenkanons sind ebenfalls die Implementierung, Aufrechterhaltung und Weiterentwicklung einer Datenschutz-Governance-Struktur. Überdies bzw. vielmehr zunehmend gerät eine bestehende gute Datenschutz-Compliance zu einem wichtigen unternehmerischen Reputationsaspekt: „Verlorene" sensitive Daten, Datenlecks mit der Folge im Internet „herumgeisternder" personenbezogener Daten, unverhältnismäßige arbeitgeberseitige Überwachungsmaßnahmen der Belegschaft oder Hackerangriffe aufgrund systembedingter IT-Schwachstellen sorgen für große mediale Beachtung und enden überdies regelmäßig in Bebußungen durch die datenschutzrechtlichen Aufsichtsbehörden gem. Art. 83 DSGVO in aufsehenerregenden Höhen. Fünfstellige Geldbußen sind an der Tagesordnung, sechsstellige Geldbußen keine Seltenheit mehr.

Daneben nimmt auch die Inanspruchnahme von Unternehmen durch Klagen auf immateriellen Schadensersatz wegen Datenschutzverstößen durch Individualpersonen zu. Eine Klageindustrie für Massenklagen formt sich bereits. Anwälte treten werbend mit Angeboten entsprechender Interessenvertretungen am Markt auf, um potentielle Anspruchsteller „einzusammeln". Aus Klägersicht praktikabel und recht einfach möglich macht dies Art. 82 DSGVO, wonach immaterieller Schadensersatz nahezu bereits für jedwede Verletzung datenschutzrechtlicher Vorgaben geltend gemacht werden kann. Zwar hat der EuGH in einigen Entscheidungen den Anwendungsbereich der Norm etwas zurückgeschnitten, in dem die Luxemburger Richter den Nachweis eines konkreten Schadens einfordern (EuGH, Urt. v. 4.5.2023 – C-300/21). Eine Bagatellgrenze darf es aber weiterhin nicht geben (EuGH, Urt. v. 14.12.2023 – C-456/22), so dass auch der bloße Kontrollverlust über die eigenen Daten einen ersatzfähigen immateriellen Schaden darstellen kann (EuGH, Urt. v. 14.12.2023 – C-340/21).

Mit zwei jüngeren Urteilen (EuGH, Urt v. 20.6.2024 – C-590/22 sowie verb. Rs. C-182/22 und C-189/22) bestätigt der EuGH diese Linie: Ein Verstoß gegen die DSGVO allein begründet zwar weiterhin keinen Schadensersatz, ein konkreter Schaden muss also folglich dargelegt werden. Allerdings reicht dafür bereits „die Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen diese Verordnung an Dritte weitergegeben wurden, ohne dass nachgewiesen werden kann, dass dies tatsächlich der Fall war […], sofern diese Befürchtung samt ihren negativen Folgen ordnungsgemäß nachgewiesen ist". Mit anderen Worten: Eine glaubhaft dargelegte Furcht allein kann ausreichen, um Schadensersatzansprüche zu begründen, es muss nicht wirklich etwas „passieren". Immerhin betont der EuGH, dass der Schadensersatz keinen abschreckenden Charakter hat, sondern „ausschließlich eine Ausgleichsfunktion erfüllt", so dass der Schweregrad und die Frage der Vorsätzlichkeit bei der Bemessung des Schadensersatzes nicht berücksichtigt werden müssen. Demnach dürfen nationale Gerichte die fehlende Schwere eines Schadens durch die Verurteilung zur Zahlung eines geringfügigeren Schadenersatzanspruchs berücksichtigen.

Für Unternehmen ist dies aber allenfalls ein sehr kleiner Lichtblick am datenschutzrechtlichen Entschädigungshorizont. Das Risiko der Inanspruchnahme wegen behaupteter Datenschutzverstöße und vermeintlicher daraus resultierender Schäden bleibt bestehen. Rechtssicherheit in Form einer praktischen Begrenzung ausufernder Entschädigungsansprüche wird nur die nationale Rechtsprechung herbeiführen können. Diese ist von einer einheitlichen Linie aber noch weit entfernt und zeichnet sich derzeit eher durch einen „kasuistischen Wildwuchs" aus. Die einzige Strategie der Risikomitigierung für Unternehmen ist es daher, den Datenschutz ernst zu nehmen und im Rahmen einer guten Corporate Governance zu einer prioritären Aufgabe der Unternehmenscompliance zu machen. Wie für andere bedeutende Compliance-Themen in Unternehmen (u.a. Anti-Corruption) gilt es damit auch für den Datenschutz ein effektives Management-System zu implementieren und fortlaufend weiterzuentwickeln.

Prof. Dr. Michael Fuhlrott

Prof. Dr. Michael Fuhlrott ist Partner bei FUHLROTT Arbeitsrecht in Hamburg. Er berät Unternehmen zu sämtlichen individual- und kollektivrechtlichen Fragestellungen mit einem Schwerpunkt im Arbeitnehmerdatenschutz.

Roto
Window & Door
Technology

Für unser Team am Standort Leinfelden-Echterdingen suchen wir ab sofort einen

Compliance Manager/Syndikusrechtsanwalt mit Schwerpunkt Compliance m/w/d

Das erwartet Sie

- Beratung der Geschäftsführung & Unterstützung der globalen Tochtergesellschaften bei allen Compliance relevanten Themen
- Weiterentwicklung des Compliance-Management-Systems
- Mitwirkung bei der Identifizierung etwaiger Compliance-Risiken und Unterstützung bei der Implementierung risikominimierender Maßnahmen
- Implementierung und Weiterentwicklung eines globalen Rechtskatasters
- Erstellung und Umsetzung verbindlicher Compliance-Richtlinien, -Dokumentationen und -Prozessen sowie Compliance-Berichterstattung
- Durchführung von Workshops, Schulungen und Unterweisungen sowie die Förderung der Compliance-Kultur und des Compliance-Bewusstseins

Das bringen Sie mit

- Erfolgreich abgeschlossenes 2. Staatsexamen zum Volljuristen mit gutem Examina oder vergleichbare Qualifikation
- Mindestens drei Jahre einschlägige Praxiserfahrung
- Integrität und Eigeninitiative, ausgeprägte Kunden- und Zielorientierung
- Verhandlungssichere Englischkenntnisse
- Ausgeprägtes analytisches und unternehmerisches Denken

Das bieten wir

- Mobiles Arbeiten
- Flexible Arbeitszeit
- Job-Rad & ÖPNV-Ticket
- Betriebsrestaurant
- Weiterbildung uvm.

Roto Frank Fenster- und Türtechnologie GmbH
Human Resources
Wilhelm-Frank-Platz 1
70771 Leinfelden-Echterdingen
ftt.roto-frank.com

Zum Roto Job Portal

www.jobs.roto-frank.com

BaFin-Razzia gegen Betreiber von Krypto-Automaten

In einer deutschlandweiten Aktion stellte die Finanzaufsicht BaFin am 20. August 2024 Krypto-Automaten sicher, an denen Bitcoin und andere Krypto-Werte gehandelt werden konnten. Wie die Behörde mitteilt, wurde dabei Bargeld in Höhe von einer knappen Viertelmillion Euro einbehalten. Die 13 beschlagnahmten Geräte wurden ohne die erforderliche Erlaubnis der BaFin betrieben und hätten zur Geldwäsche genutzt werden können.

© IMAGO / Eckhard Stengel

Ein Bitcoin-Laden in Bremen: Hier konnten an Automaten Euros in Internetwährung umgetauscht werden. Auf Anweisung der Bafin wurde der Betrieb aber schon im März 2020 eingestellt.

An insgesamt 35 Standorten gingen Beamte der BaFin mit Unterstützung von Polizei und Deutscher Bundesbank sowie in Abstimmung mit dem Bundeskriminalamt (BKA) gegen die Aufsteller vor und sammelten mit rund 60 Einsatzkräften die illegal betriebenen Automaten ein.

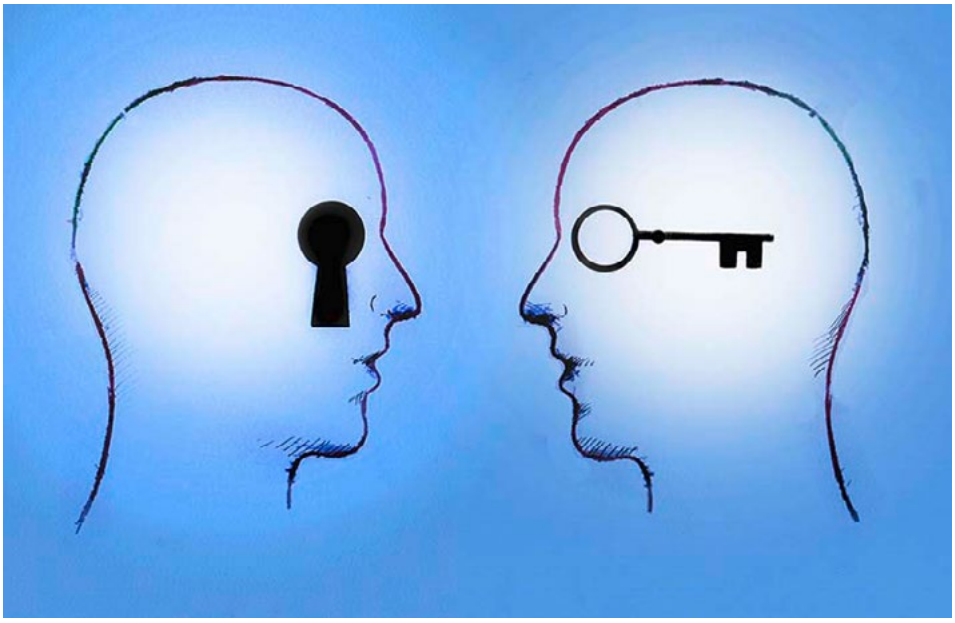
„Das Wechseln von Euro in Krypto-Währungen und umgekehrt stellt gewerbsmäßigen Eigenhandel oder ein Bankgeschäft dar und benötigt deshalb laut Gesetz (§ 32 Kreditwesengesetz) die ausdrückliche Erlaubnis der BaFin. Andernfalls wird das Geschäft illegal betrieben", stellt die Behörde in einer Mitteilung zur Razzia klar. Die Erlaubnispflicht schütze sowohl die Integrität des Finanzsystems als auch Verbraucherinnen und Verbraucher. Mit dem Handel mit Krypto-Werten seien erhebliche Risiken bis hin zum Totalverlust verbunden. Illegal handelnde Betreiber würden daher von Polizei und Staatsanwaltschaft strafrechtlich verfolgt, den Tätern drohen bis zu fünf Jahre Freiheitsentzug.

Manche Wechselautomaten zögen zudem Nutzer mit kriminellen Absichten an, warnt die BaFin. Wer Krypto-Automaten betreibt, müsse zur Geldwäscheprävention die Identität der Kunden feststellen, entweder beim Start der Geschäftsbeziehung oder wenn die Kunden außerhalb einer Geschäftsbeziehung Werte von 1.000 Euro oder mehr wechseln. Generell gelte: „Werden Anhaltspunkte für die illegale Herkunft des Geldes oder der Zusammenhang mit Terrorismusfinanzierung festgestellt, muss dies an die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) gemeldet werden. Tauschautomaten, an denen diese Sorgfaltspflichten nicht eingehalten werden, eignen sich aufgrund der Anonymität zur Geldwäsche."

chk

Kolumne: Spielräume erkennen

In den vorherigen Ausgaben hat unser Kolumnist Markus Jüttner den Begriff des „Systems" für die Compliance näher beleuchtet, insbesondere was ein Compliance-System von einem Compliance-Haufen unterscheidet und wann man von einem integrierten Compliance-Management-System (CMS) sprechen kann. Ein bedeutsamer Blickwinkel wurde aber noch nicht betrachtet, nämlich der Kontext.



Spielräume erkennen: Compliance-Verantwortliche müssen immer zwei Systeme im Blick haben – das CMS und die Organisation.

Auch das formal beste CMS ist unwirksam, wenn der Kontext, in dem es eingesetzt wird, nicht berücksichtigt wird. Dieser Kontext ist – wenig überraschend – die jeweilige nationale oder gar internationale Organisation, die regel- und gesetzeskonform ihre Ziele erreichen will und muss. Dabei wäre es ungenügend, die Organisation lediglich aus der juristischen Perspektive (Betrieb, Verband, AG, GmbH, Konzern etc.), der betriebswirtschaftlichen (Auf- und Ablauforganisation) oder aus der psychologischen (Ansammlung bzw. Ort von mehreren Individuen) zu betrachten; denn die jeweilige Organisation selbst ist ein System, jedoch im Gegensatz zum CMS und den einschlägigen Gesetzen ein dynamisches, soziales System, das zudem komplex ist.

So sind Unternehmen weder „einfach" beziehungsweise „kompliziert" aufgebaut wie etwa eine Maschine, eine Uhr o.ä., bei der absehbar ist, wenn etwas geändert wird, was dann passiert. Ein Unternehmen ist nicht linear-kausal, dessen Verhalten sich berechnen oder prognostizieren lässt; die Organisationswissenschaften sprechen in diesem Zusammenhang von Emergenz. Manager und Berater sehen entgegen dieser Erkenntnis weiterhin vielfach Organisationen als (komplizierte) Maschinen an, die mit standardisierten Prozessen und Richtlinien zu steuern seien; insofern wird Compliance auch mit einem Schachspiel verglichen. Aber nicht nur der inzwischen verstorbene James March und seine Kollegen haben gezeigt, dass die Vorgänge und Entscheidungen in Organisationen mitnichten den vorgezeichneten Programmen und Regeln folgen. Dahinter steckt keine böse Absicht, sondern es ist Konsequenz komplexer, emergenter, sozialer Systeme.

So werden zwar „kompliziert" und „komplex" im Management- und Compliance-Alltag unbedacht synonym verwendet, allerdings ist kompliziert nicht die kleine Schwester von komplex (Habermann/Schmidt 2021). Der Kern in der Unterscheidung liegt in der Vorhersagbarkeit und Kausalität. „Die Grenze zwischen kompliziert und komplex verläuft also zwischen vorhersagbar und überraschend, zwischen statisch und dynamisch und letztlich zwischen tot und lebendig. Der erfolgreiche Umgang mit Komplexität bedingt einen Wechsel der Methode von der Analytik zur Empirie. Verhalten und Kausalitäten lassen sich nicht mehr rein analytisch durch Zerlegen in Komponenten bestimmen, sondern können nur über geeignete Hypothesen und Experimente zu ihrer Verifikation oder Falsifikation verstanden und beschrieben werden." (Raitner 2021)

Insofern wird verständlicher, warum Compliance in der Praxis so schwierig zu managen ist. Ein CMS und das jeweils in den Blick genommene Gesetz, was es einzuhalten gilt, sind, wenn nicht einfach dann lediglich kompliziert. Die Organisation, in der das CMS wirken soll, ist hingegen komplex. Maßnahmen und Vorkehrungen, die für einfache bzw. komplizierte Kontexte geeignet sind, passen aber nicht für komplexe Situationen. Das zeigt sich beispielsweise in der Compliance-Risikoanalyse; häufig kommen hier Konzepte und Methoden des konventionellen Risikomanagements zur Anwendung, die für statische, komplizierte Risiken aber eben nicht für dynamische, komplexe Unsicherheits-Zusammenhänge geeignet sind. Die simplifizierten 3x3- bzw. 4x4-Risikomatrixen zeigen dies. Kombiniert man die Analyse mit Detailverliebtheit einerseits und waghalsigen Annahmen andererseits, reichert es mit quantitativen Eintrittswahrscheinlichkeiten, Durchschnittsbildungen an, blendet man Unsicherheit aus und verweigert man sich einer Methodenvielfalt, darf man sich nicht wundern, dass die Compliance-Risikoanalyse mit der realen Organisation und den darin stattfindenden Verhalten und tatsächlich getroffenen Entscheidungen wenig zu tun hat.

Compliance-Management ist somit letztlich nur dann wirksam, wenn es Teil des sozialen Systems ist, d.h. im Kontext von Entscheidung, Informalität, Mitgliedschaft und Vernetzung stattfindet. Das gegenwärtige Compliance-Managementverständnis lässt diesen Zusammenhang häufig außen vor. Compliance-Management wird mit planerischem Organisieren gleichgesetzt (instrumenteller Organisationsbegriff). Übersehen wird, dass das Unternehmen eine Organisation ist (institutioneller Organisationsbegriff). Compliance-Management weist ohne ein entsprechendes Verständnis des Unternehmens als komplexes soziales System idealistische und fiktive Züge auf, sowohl in der Zielsetzung, in der Planung als auch in der Wahl der Mittel. Wirksames Compliance-Management bedarf daher statt einer impliziten Gleichsetzung mit Organisieren (im Sinne planerischen Handelns) eines Organisationsverständnisses (als soziales System). Insoweit hat ein Compliance-Verantwortlicher letztlich immer zwei Systeme zu managen und im Blick zu haben: Das CMS als juristisch-betriebswirtschaftliches System und seine Organisation als soziales System. Wirksame Compliance-Programme legen damit auch den Fokus „eher auf das Verhalten als auf Gesetze sowie Vorschriften und beobachten vor allem die Worte und Handlungen ihrer eigenen Mitarbeiter. Sie fragen sich immer wieder nach dem Warum und Wie und wollen wirklich wissen, was in ihren Unternehmen vor sich geht." (Chen 2017) *Markus Jüttner*

Markus Jüttner ist Rechtsanwalt und Partner des Fachbereichs Forensic & Integrity Services, Ernst & Young GmbH. Er berät Unternehmen in Fragen der Compliance, der Kultur und der Integrität.
markus.juettner@de.ey.com

Ihr DSB-Praxiswebinar

Microsoft 365: Praktische Lösungen zum Datenschutz

17. Oktober 2024 | 9.00 - 13.30 Uhr | Webinar

09:00 Uhr **Begrüßung**

09:10 Uhr **Herausforderungen beim Einsatz von M365**
- M365 und die Transformation von Software-Versionen zu SaaS: Folgen für Compliance und interne Freigabe
- Ausführliche Darstellung der Kritik und Unterstützung seitens der Datenschutzaufsicht (insb. DSK, Landesdatenschutzbeauftragte, EDSB)

09:50 Uhr **Argumentationen für einen Einsatz von M365 in privaten und öffentlichen Stellen**
- Die Aufsichtsbehörden, DSK und Einordnung in die Exekutive
- Was besagt das Vertragswerk zu M365 – was sind Product Terms und DPA, wofür gelten sie und was besagen sie?
- Entgegnungen zur Kritik und Vorschlägen der ASB
- Restrisiken aus datenschutzrechtlicher Unklarheit und Business Judgement Rule

10:30 Uhr **Einführung von M365 bei „Die Autobahn GmbH des Bundes“**
- Werkstattbericht: Einführung von M365 bei „Die Autobahn GmbH des Bundes“ – Herausforderungen und Best Practices
- Podiumsdiskussion: Zwischen Projektmanager und Kontrolleur – Die Rolle des Datenschutzes beim Rollout von M365

11:10 Uhr **Pause**

11:20 Uhr **Insights in die Microsoft-Welt und ihre Compliance-Aspekte**
- Die verschiedenen Microsoft-Lizenzen, ihre Bezugswege und Auswirkungen auf Ihre Compliance
- EU Data Boundary, Customer Lockbox und weitere Datensicherheits-Dienste von Microsoft
- Überblick: Copilot-Varianten, M365 Copilot und Datenschutz
- Datenschutz-Folgenabschätzung in der Praxis

12:00 Uhr **Besondere Anwendungsfälle**
- M365 in öffentlichen Stellen und im Bildungsbereich
- § 203 StGB und andere Geheimhaltungsnormen; die Berufsgeheimnisträger-Zusatzvereinbarung von Microsoft
- Betriebsrat/Personalrat und Kollektivvereinbarungen
- Das aktuelle Thema des Monats *(wird kurz vor dem Webinar bekanntgegeben)*

13:00 Uhr **Diskussions-/Fragerunde mit allen Referierenden + Teilnehmenden**

13:30 Uhr **Ende**

Dr. Stefan Brink
Wissenschaftliches Institut für die Digitalisierung der Arbeitswelt

Dr. Olaf Koglin
LegalCheck

Raphael Köllner
KöllnService GmbH

Wiebke Löck
Die Autobahn GmbH des Bundes

Ihr Ansprechpartner:
Jasha Baniashraf
E-Mail: jasha.baniashraf@dfv.de
Tel.: +49 69. 75 95 - 27 73

Teilnahmegebühr (zzgl. MwSt.):
199,– EUR Abonnenten DSB & Behördenvertreter
299,– EUR regulär

Eine Veranstaltung von
DATENSCHUTZ-BERATER

JETZT QR-CODE SCANNEN UND DIREKT ANMELDEN!
oder unter www.ruw.de/microsoft

Kontakt: Deutscher Fachverlag GmbH · Jasha Baniashraf
Mainzer Landstraße 251 · 60326 Frankfurt · Tel: 069 7595-2773 · jasha.baniashraf@dfv.de

dfv Mediengruppe

Die Implementierung eines KI Governance Frameworks

Es ist inzwischen keine Frage mehr, ob KI in einem Unternehmen eingesetzt wird, sondern vielmehr in welchem Umfang und welche Bereiche und Prozesse betroffen sind. Der Einsatz von KI bringt allerdings auch regulatorische und ethische Risiken mit sich, denen sich Unternehmen stellen müssen. Um diese Risiken zu steuern, aber auch um den zukunftsorientierten Einsatz von KI sicherzustellen, bedarf es innerhalb eines Unternehmens Leitlinien und Handlungsrahmen für Nutzer und Betreiber von KI-basierten Anwendungen. In diesem Beitrag beschäftigt sich Eric S. Soong mit der Frage, wie ein solcher Handlungsrahmen bzw. ein KI Governance Framework aus Sicht einer Compliance-Organisation in einem Industrieunternehmen aussehen kann.

© IMAGO / Westend61

Integration von KI: Hierbei müssen im Unternehmen mehrere Kräfte zusammenspielen.

Unabhängig davon, ob in einem Unternehmen bereits KI-Expertise vorhanden ist oder diese teuer eingekauft werden muss, stellt sich zunächst die Frage, welche Organisationseinheit(en) innerhalb eines Unternehmens die Verantwortung für die KI Governance innehaben sollte(n). Die mit KI verbundenen Risiken betreffen eine Vielzahl an Abteilungen und Prozessen in einem Unternehmen. Ein KI Governance Framework erfordert somit das interdisziplinäre Zusammenspiel verschiedener Fachbereiche. Erforderlich ist daher ein modernes Risikomanagementsystem, das die verschiedenen Risiken unternehmensweit identifiziert, bewertet und steuert sowie eine Verbindung der Risiken berücksichtigt. Die Compliance-Funktion kann dabei aufgrund ihrer Erfahrungen aus den unter den klassischen Compliance-Begriff fallenden Themenfeldern eine wesentliche Rolle spielen, um dieses neue technische Themenfeld zu erfassen.

Da die meisten Compliance-Funktionen aber eher mit Juristen und Betriebswirten und nicht mit KI-Experten besetzt sein dürften, muss die Rolle der Compliance-Funktion in diesem Zusammenhang als beratende, koordinierende und konsolidierende Instanz, die auf eine interdisziplinäre Zusammenarbeit und einen adäquaten Informationsaustausch sowie die Herbeiführung von schnellen Entscheidungen hinwirkt, verstanden werden. Dieser interdisziplinäre Ansatz fördert eine holistische Betrachtung der entstehenden Risiken sowie eine leichtere Mitigation derselben.

Aber auch aus Sicht der Unternehmensleitung empfiehlt es sich, diese herausfordernde Aufgabe an eine Compliance-Funktion zu delegieren, da es die originäre Aufgabe einer Unternehmensleitung ist, die von ihr verantworteten, unternehmerischen Aktivitäten in einer Art und Weise zu organisieren und zu überwachen, dass sie mit den jeweils anwendbaren straf- und bußgeldbewehrten Gesetzen in Einklang stehen.

Bei der konkreten Ausgestaltung des KI Governance Frameworks sollte zunächst darüber nachgedacht werden, das KI Governance Framework in bereits im Unternehmen vorhandene DS-GVO- oder IT-Sicherheits-Compliance-Strukturen zu integrieren bzw. diese zu nutzen. Fundament des Governance Frameworks stellt eine entsprechende Richtlinie dar, die zentrale KI-Leitlinien, Grundsätze sowie Vorgaben für deren Umsetzung definiert. Sie sollte die Werte aus dem Unternehmenskodex wie auch interne Regulatorik widerspiegeln und als gemeinsame Grundlage für den Umgang mit KI dienen. Essenzieller Bestandteil der Richtlinie sollten Leitlinien sein, die sowohl die Potentiale von KI als auch die Risiken bei deren Einsatz steuern. Ein rein risikoorientierter Ansatz, der ausschließlich Gefahren thematisiert, könnte gegebenenfalls bremsend auf den KI-Reifegrad einwirken, Innovation verlangsamen oder Mitarbeitende verunsichern. Auch empfiehlt es sich, zunächst auf der Ebene von Grundsatzprinzipien/ Guiding Principles einen Handlungsrahmen für die Nutzung von KI-Anwendungen vorzugeben. Dieser sollte Hinweise darauf enthalten, dass die Anwendungen nur mit gesicherter Internetverbindung genutzt und die Datenschutzrichtlinien sowie die allgemeinen Geschäftsbedingungen der jeweiligen Anwendung beachtet werden. Ferner, dass Daten zu anonymisieren und Ergebnisse auf Genauigkeit und Plausibilität zu prüfen sind.

Mit Blick auf die Zukunft bleiben die Aussichten für die Steuerung der KI in der EU herausfordernd. Hinzu kommen Regulierungsansätze aus anderen Rechtskreisen, wie den USA oder China. Da sich die KI-Technologien rasant weiterentwickeln, müssen auch geschaffene Governance-Strukturen flexibel und anpassungsfähig bleiben, kurz robust, um neuen Entwicklungen und unvorhergesehenen Risiken zu begegnen. Ein „One size fits it all"-Ansatz erscheint daher weniger realistisch. Zuletzt bietet die digitale Transformation durch KI aber auch die Möglichkeit, präventive, detektierende und reagierende Maßnahmen neu zu gestalten, zu verschlanken und effizienter zu machen. Compliance muss sich dadurch zwar einerseits um neue Risiken kümmern, kann jedoch andererseits die mit KI entstehenden Chancen auch für die eigene Arbeit nutzen.

Eric S. Soong

© Schaeffler

Eric S. Soong ist seit 2014 Group Chief Compliance Officer & Head of Corporate Security der Schaeffler Gruppe. Er ist weltweit für verschiedene Governance-Funktionen im Unternehmen verantwortlich, hierzu zählt u.a. der Bereich Compliance. Er ist zudem in der Herausgeberschaft des Compliance-Beraters.

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662
Geschäftsführung: Peter Esser (Sprecher), Sönke Reimers (Sprecher), Thomas Berner, Markus Gotta
Aufsichtsrat: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Ruß
Redaktion: Christina Kahlen-Pappas (verantwortlich),
Telefon: 069 7595-1153, E-Mail: christina.kahlen-pappas@dfv.de
Verlagsleitung: RA Torsten Kutschke,
Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Matthias Betzler,
Telefon: 069 7595-2785, E-Mail: Matthias.Betzler@dfv.de
Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Berneis Legal & Compliance; Ralf Brandt, LTS Lohmann Therapie-Systeme AG / Drug Delivery Systems Beteiligungs GmbH; Joern-Ulrich Fink, Central Compliance Germany, Deutsche Bank AG; James H. Freis, Jr., Chief Compliance Officer, Deutsche Börse AG; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Corina Käsler, Head of Compliance, State Street Bank International GmbH; Olaf Kirchhoff, Schenker AG; Torsten Krumbach, msg Systems AG; Dr. Karsten Leffrang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Muth-zur-Entwicklung; Stephan Niermann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, BSH Hausgeräte GmbH; Hartmut T. Renz, Citi Chief Country Compliance Officer, Managing Director, Citigroup Global Markets Europe AG; Dr. Barbara Roth, Chief Compliance Officer, UniCredit Bank AG; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Elena Späth, AXA Assistance Deutschland GmbH; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen; Heiko Wendel, Rolls-Royce Power Systems AG; Dietmar Will, Audi AG.
Jahresabonnement: kostenlos
Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)
Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de

1. Deutscher Beschäftigtendatenschutztag

Donnerstag, 24. Oktober 2024 | München

Eine Veranstaltung von DATENSCHUTZ-BERATER und POELLATH

Mittwoch, 23. Oktober 2024

ab 19.00 Uhr Get-Together im Ratskeller München
Marienplatz 8, 80331 München

Donnerstag, 24. Oktober 2024

Ab 8.30 Uhr Registrierung

09.00 Uhr **Begrüßung & Einführung**
Torsten Kutschke, dfv Mediengruppe
Dr. Dominik Sorber, POELLATH
Dr. Michaela Felisiak, Eversheds Sutherland

09.15 Uhr **Fokus Bußgelder: Unbegrenzte Unternehmenshaftung für Datenschutzverstöße?**
Dr. Isabelle Brams, Latham & Watkins

09.50 Uhr **Trends und weiße Flecken im Beschäftigtendatenschutz aus Sicht der Aufsichtsbehörde und der Anwaltspraxis**
Dr. Dominik Sorber, POELLATH
Miriam Meder, Bayerisches Landesamt für Datenschutzaufsicht

10.40 Uhr **Kaffee- und Kommunikationspause**

11.15 Uhr **Bußgelder im Beschäftigtendatenschutz – die Blacklist und die Bußgelder**
Bonnie Silverman, Referentin Berliner Beauftragte für Datenschutz und Informationsfreiheit

11.50 Uhr **Erforderlichkeit bei Amazon – eine Frage der DSGVO?**
Hans-Hermann Schild, Vorsitzender Richter am VG i.R., Kassel

12.25 Uhr **Aufhebungsvertrag, gerichtlicher Vergleich und Verzicht auf den Auskunftsanspruch?**
Christina Knoepffler, Rechtsanwältin

13.00 Uhr **Mittagspause**

14.00 Uhr **Interaktives Format**
Maria Christina Rost, Landesbeauftragte für den Datenschutz des Landes Sachsen-Anhalt
Moderation: Dr. Michaela Felisiak und **Dr. Dominik Sorber**

14.35 Uhr **Wann ist der Auskunftsanspruch rechtsmissbräuchlich?**
Barbara Thiel, Die Landesbeauftragte für den Datenschutz Niedersachsen a. D.

15.10 Uhr **AI Governance und aktuelle Unternehmensherausforderungen**
Johannes Hübler, Novartis Pharma AG

15.45 Uhr **Kaffee- und Kommunikationspause**

16.15 Uhr **Schadensersatzansprüche und die arbeitsgerichtliche Rechtsprechung – Eine praktische Zwischenbilanz**
Alexander Dubon, Richter am Arbeitsgericht Würzburg

16.50 Uhr **Schadensersatzansprüche ohne Darlegung eines Schadens?**
Prof. Dr. Jan Eichelberger, Leibniz Universität Hannover

17.25 Uhr **Zusammenfassung & Ausblick**
Dr. Dominik Sorber

Im Anschluss: Veranstaltungsausklang mit Fingerfood & Drinks


Torsten Kutschke


Dr. Dominik Sorber


Dr. Michaela Felisiak


Dr. Isabelle Brams


Miriam Meder


Bonnie Silverman


Hans-Hermann Schild


Christina Knoepffler


Maria Christina Rost


Barbara Thiel


Johannes Hübler


Prof. Dr. Jan Eichelberger

Anmeldung 1. Deutscher Beschäftigtendatenschutztag

Lena Wehrmann
Projektmanagerin
E-Mail: Lena.Wehrmann@dfv.de
Tel: 069. 7595-2784
Fax: 069. 75 95-1150

Deutscher Fachverlag GmbH
Fachmedien Recht und Wirtschaft
Mainzer Landstraße 251
60326 Frankfurt

JETZT QR-CODE SCANNEN UND DIREKT ANMELDEN!
oder unter www.ruw.de/dbdt

Hinweisgeberschutz: Vom Pflichtprogramm zur strategischen Chance

Das Hinweisgeberschutzgesetz (HinSchG), das im Juli 2023 in Deutschland in Kraft trat, markierte einen wichtigen Meilenstein für den Schutz von Whistleblowern, die Schaffung sicherer Meldewege und die Aufarbeitung von Missständen in Unternehmen. Ein Jahr nach seinem Inkrafttreten ist der Anteil der Unternehmen, die ein Hinweisgebersystem eingeführt haben, laut EQS Whistleblowing-Umfrage 2024 von 82 Prozent auf ganze 97 Prozent gestiegen.

Haken dran? Die Umsetzung des Whistleblower-Schutzes ist nur ein erster Baustein.

Das HinSchG hat den Druck auf Unternehmen erhöht – nicht zuletzt, da die zuständigen Behörden nun verstärkt bei ihnen nachfragen werden, ob sie die Vorgaben umgesetzt haben. Die Umfrage zeigt: Gesetzeskonformität war der größte Treiber für die Einführung von Hinweisgebersystemen – 94 Prozent der Unternehmen gaben dies als Grund an.

Vor Inkrafttreten des HinSchG beklagten gerade kleinere Unternehmen den potenziell hohen Umsetzungsaufwand. Nach der Implementierung einer Meldestelle müssen schließlich auch langfristig Ressourcen für die Bearbeitung von Hinweisen bereitstehen. Ein Fünftel der Unternehmen in der EQS-Umfrage erhielt im vergangenen Jahr immerhin mehr als zehn Meldungen, denen sie nachgehen mussten. Abhilfe schaffen digitale Tools, die wesentlich zu einer zügigen Bearbeitung beitragen. So setzen z.B. bereits 74 Prozent der Unternehmen auf Softwaresysteme. Diese ermöglichen es, den gesamten Prozess, von der Bearbeitung der Erstmeldung bis zur Kommunikation mit dem Whistleblower, effizient zu gestalten.

Ein zentraler Vorteil digitaler Lösungen ist die Möglichkeit, Anonymität für Whistleblower zu gewährleisten. Über eine Pflicht dazu hat der Gesetzgeber debattiert und sie schließlich aus dem Gesetzestext gestrichen. Ob das sinnvoll war, ist diskutabel, aber die Realität zeigt: Unternehmen haben längst verstanden, dass sie langfristig profitieren, wenn sie anonyme Meldekanäle anbieten, und neun von zehn tun dies auch bereits. Laut früheren EQS-Studien werden 50 Prozent der Meldungen anonym gegeben, wenn diese Option besteht. Gibt es sie nicht, wenden sich Whistleblower eher an externe Meldestellen von Behörden. Liegt eine Meldung erst einmal bei einer externen Stelle, hat das Unternehmen keine Kontrolle mehr über ihre Aufarbeitung.

Damit ein Whistleblowing-System seinen Zweck erfüllen kann, dürfen sich Unternehmen aber nicht auf einer technischen Lösung ausruhen. Es braucht vor allem eine Unternehmenskultur, in welcher der Schutz von Whistleblowern aktiv gefördert wird. Mitarbeitende fühlen sich nur dann ermutigt, Missstände zu melden, wenn sie darauf vertrauen können, dass ihre Hinweise ernst genommen werden und sie keine Repressalien fürchten müssen. Eine starke Meldekultur war für Unternehmen in der EQS-Umfrage nach Compliance der zweitwichtigste Grund für die Einführung eines Hinweisgebersystems.

Marcus Sultzer ist Mitglied des Vorstands der EQS Group und als Chief Revenue Officer verantwortlich für den Bereich Globale Umsätze und Marketing.

Mehr noch als das Meldesystem spielt dabei die Haltung von Führungskräften – bis hin zur Geschäftsführung – eine zentrale Rolle. Sie haben eine Vorbildfunktion und müssen aktiv zu einer Kultur beitragen, in der Offenheit und Transparenz gelebt werden. Dazu gehört auch, proaktiv zu kommunizieren, welche Kanäle für Hinweisgeber zur Verfügung stehen. Bei der Kommunikation sehen wir in der Praxis oft noch Nachholbedarf. Selbst kleine Unternehmen erhalten typischerweise mehrere Hinweise pro Jahr. Ist dies nicht der Fall, sollte das als Warnsignal verstanden werden: Möglicherweise bestehen Missstände unerkannt und kommen erst ans Licht, wenn bereits ein hoher Schaden entstanden ist.

Stehen die richtigen Meldekanäle zur Verfügung, und sind sie den Mitarbeitenden bekannt? Wenn nicht, was muss getan werden, um dies zu verbessern und auch das Vertrauen in ihre Wirksamkeit zu stärken? Damit investieren Unternehmen in eine loyale und engagierte Belegschaft, die Probleme anspricht, bevor sie eskalieren.

Mit Inkrafttreten des HinSchG haben sich Unternehmen auf die zügige Umsetzung konzentriert. Whistleblowing allein macht aber noch keine Compliance-Kultur aus, sondern ist nur ein – wenn auch wichtiger – Baustein. Es gilt jetzt, stärker über einzelne Gesetze hinauszudenken: In einer komplexen Compliance-Landschaft müssen Unternehmen einen ganzheitlichen, integrativen Ansatz mit klaren Richtlinien und Prozessen entwickeln, der durch eine digitalen Lösung unterstützt wird.

Wer Compliance nicht als lästige Pflicht, sondern als Kern der strategischen Ausrichtung begreift, minimiert nicht nur das Risiko rechtlicher Konsequenzen, sondern stärkt auch nachhaltig die Unternehmensreputation. Für Compliance-Verantwortliche bedeutet das: Ihre Arbeit geht inzwischen weit über die Umsetzung gesetzlicher Vorgaben hinaus. Sie tragen maßgeblich dazu bei, den Erwartungen von Mitarbeitenden, Kunden oder Investoren gerecht zu werden und das Vertrauen der Öffentlichkeit in das Unternehmen zu stärken. Dieses Vertrauen wird in der globalen Geschäftswelt immer mehr zum wichtigsten Kapital. Compliance ist damit nicht nur ein unverzichtbarer Bestandteil verantwortungsvoller Führung – sie wird zum Schlüsselfaktor für den langfristigen Unternehmenserfolg.

Marcus Sultzer