



Inhalt



© IMAGO / Panthermedia

Aufmacher

Im toten Winkel der Aufsicht

Über 300 Banken sind von Geldwäscheprüfungen befreit. Für Dr. Marcus Sonnenberg ist das ein unbeabsichtigter „blinder Fleck der Aufsicht“. Das Ansehen des Finanzstandorts Deutschland, warnt er in unserem Aufmacher, könnte dadurch erneut schweren Schaden nehmen.

2

Recht

Praxis

News



© Pixabay

4

Neobanken – Regelungslücke im Aufsichtsrecht?

Die Bedeutung sogenannter Neobanken auf dem Bankenmarkt nimmt stetig zu. Die Geschäftsmodelle sowie die rechtlichen Konstrukte dieser unter dem Titel Neobanken, aber auch Challenge-Banken, Online-Banken, Internet-only-Banken, virtuelle oder digitale Banken geführten Institute stellen die Aufsicht vor Herausforderungen.

6 Online-Anbieter müssen nicht immer über Herstellergarantien informieren



© Maurice Kohl

8

BaFin: „Finanzstabilität ist kein Selbstläufer“

Zur Jahrespressekonferenz der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) am 3. Mai 2022 stellte ihr Präsident, Mark Branson, insbesondere die Risiken für das deutsche Finanzsystem und dessen Stabilität heraus.

8 Neue Grundsätze der Zusammenarbeit

10 Hinweisgebersystem im Mittelstand: so viel wie nötig, so wenig wie möglich



© IMAGO / ZUMA Wire

12

EuG bestätigt EZB-Beschluss: Keine Bank-Beteiligung für Berlusconi

Aufgrund seiner Verurteilung wegen Steuerbetrugs im Jahr 2013 erfülle Silvio Berlusconi nicht die für Inhaber von qualifizierten Beteiligungen geltende Anforderung an den Leumund, beschied das Gericht der Europäischen Union (EuG) Mitte Mai und untersagte damit dem ehemaligen italienischen Ministerpräsidenten den Erwerb einer qualifizierten Beteiligung an Banca Mediolanum.

12 Deutsche Compliance Konferenz 2022: ein Ausblick

Geldwäsche & Recht
Alles rund um Geldwäscheprävention, Repression und Sicherheit
Hier kostenlos probelesen!
Neu!

Veranstaltungen

28. + 29.06.2022 | Frankfurt am Main oder Online | **Deutsche Compliance Konferenz**

25.-27.09.2022 | Düsseldorf oder Online | **Datenschutzkonferenz**

Im toten Winkel der Aufsicht

Über 300 Banken sind von Geldwäscheprüfungen befreit. Für Dr. Marcus Sonnenberg ist das ein unbeabsichtigter „blinder Fleck der Aufsicht“. Das Ansehen des Finanzstandorts Deutschland, warnt er in unserem Aufmacher, könnte dadurch erneut schweren Schaden nehmen.



© IMAGO / Panthermedia

Mut zur Lücken oder Fallstrick? Rund 300 Finanzinstitute sind von jeder geldwäscherechtlichen Aufsicht durch die BaFin ausgenommen.

Banken sind besonders anfällig für Geldwäsche. Nach **Einschätzung der Bundesregierung** besteht für den Bankensektor ein hohes Risiko für Geldwäsche. Auch die Skandale der letzten Jahre bestätigen dies immer wieder. So hatten bzw. haben auch eine Vielzahl an deutschen Instituten Probleme bei der Erfüllung von Geldwäschevorschriften (u.a. Deutsche Bank, Commerzbank, Wirecard, N26). Nicht immer hat dabei die BaFin als zuständige Aufsichtsbehörde rechtzeitig und effektiv eingegriffen. Insbesondere im Fall von Wirecard wurde über Jahre **nicht genau genug hingeschaut**.

Aufgrund dieser Anfälligkeit des Finanzsektors wäre anzunehmen, dass alle Banken in Deutschland einer strengen Geldwäschaufsicht unterliegen. Umso erstaunlicher ist die Tatsache, dass es eine ganze Reihe an Instituten gibt, die im Hinblick auf Geldwäsche schon seit längerer Zeit überhaupt nicht überwacht werden.

So sind rund **300 Finanzinstitute** von jeder geldwäscherechtlichen Aufsicht durch die BaFin ausgenommen. Dabei handelt es sich in der Regel um Spezialinstitute und Tochtergesellschaften von Vollbanken. Diese Akteure sind Verpflichtete nach dem Geldwäschegesetz und haben daher auch alle geldwäscherechtlichen Auflagen zu erfüllen.

Allerdings müssen sie hierüber nach außen hin keine Rechenschaft ablegen. Daher weiß auch die BaFin nicht, ob und in welchem Umfang die geldwäscherechtlichen Pflichten auch tatsächlich befolgt werden. Die Finanzaufsicht prüft auch nicht, ob die Institute angemessene Sicherungssysteme gegen sonstige strafbare Handlungen aufweisen.

Dieser blinde Fleck der Aufsicht ist nicht gezielt beabsichtigt, sondern eine Nebenfolge aus der Freistellung von der sogenannten Solvenzaufsicht. Dabei geht es um die Prüfung der Banken und Versicherungen in Hinblick auf die Aufrechterhaltung ihrer ständigen Zahlungsfähigkeit. Nach **§ 2 Abs. 4 bzw. § 2 Abs. 5 Kreditwesengesetz (KWG)** kann die BaFin in eigenem Ermessen bei unter ihrer Aufsicht stehenden Instituten von einer Überwachung absehen.

Dies führt jedoch auch dazu, dass keine Aufsicht über die Einhaltung von Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung erfolgt. Geldwäschebekämpfung und die Verhinderung von Zahlungsausfällen sind jedoch zwei völlig verschiedene Aufgaben. Nur weil bei einem Institut das Risiko für einen Ausfall der Zahlungsfähigkeit gering ist, ist es noch lange nicht immun gegen den Missbrauch

zu Zwecken der Geldwäsche und Terrorismusfinanzierung.

Die BaFin begründet die großzügige Befreiung dieser Banken mit der „Atypizität“ ihrer Geschäfte. Das mag für die Frage des Zahlungsausfallrisikos eine Rolle spielen, ist jedoch für die Prävention von Geldwäsche fatal. Geschäfte, die gerade nicht typischerweise zu Zahlungsausfällen im kritischen Bereich führen, können für Geldwäschezwecke hingegen ideal sein.

Die organisierte Kriminalität hat ein großes Interesse daran, Geld aus illegalen Quellen möglichst abseits der typischen Wege zu waschen. Bekanntermaßen ist das Erkennen und Bekämpfen von Geldwäsche ein Katz-und-Maus-Spiel. Die Methoden der Geldwäsche werden in sog. Typologiepapieren analysiert und den Verpflichteten des Geldwäschegesetzes (insbesondere den Banken) zur Verfügung gestellt. Die Unternehmen haben dann die Möglichkeit, diese Erkenntnisse zur Verbesserung ihrer Geldwäschesysteme zu nutzen. Neue Methoden entstehen daher typischerweise abseits dieser Pfade.

Ist ein Institut einmal freigestellt, verschwindet diese Bank aus dem Aufsichtsfokus, solange der Freistellungsbescheid wirksam ist. Freistellungen gelten in der Regel viele Jahre. Da in dieser Zeit keine Geldwäschaufsicht stattfindet, fehlen der BaFin auch die Erkenntnisse für eine abweichende Entscheidung in der Zukunft. Werden die befreiten Institute in der Zwischenzeit für Geldwäsche oder zur Terrorismusfinanzierung missbraucht, erfährt sie hiervon in der Regel nichts.

Problematisch ist die Entscheidung der BaFin auch aus rechtlicher Sicht. Nach den Geldwäscherichtlinien der EU führt die Freistellung von der Geldwäschaufsicht nicht dazu, dass diese Institute die entsprechenden Pflichten nicht mehr zu erfüllen haben. De facto besteht aber die Gefahr, dass diese Banken mangels externer Aufsicht keine effektive Geldwäscherprävention im Sinne des EU-Rechts betreiben. Aus diesem Grund hat die **Bürgerbewegung Finanzwende e.V. ein Vertragsverletzungsverfahren bei der EU-Kommission angeregt**. Eine Antwort der Kommission hierauf steht noch aus.

Vor diesem Hintergrund sollte sich die BaFin die Frage stellen, ob sie es sich leisten kann, die bisher freigestellten Institute weiterhin nicht zu überwachen. Käme es aufgrund dieser Untätigkeit zu einem neuen Geldwäscheskandal, würde das Ansehen des Finanzstandorts Deutschland erneut schweren Schaden nehmen.

Dr. Marcus Sonnenberg



© Dr. Marcus Sonnenberg

Dr. Marcus Sonnenberg ist Rechtsanwalt im Bereich Compliance und Mitautor des **Frankfurter Kommentars zum Geldwäschegesetz**. Daneben bildet er seit mehreren Jahren im Rahmen eines Zertifizierungslehrgangs Geldwäschauftragte im Finanzbereich aus. Privat betreut er einen Blog für Geldwäschauftragte: <https://www.hilfssheriff.de/newsletter/>

Deutsche ComplianceKonferenz 2022

28. & 29. Juni 2022 - Steigenberger Frankfurter Hof

HYBRID:
TEILNAHME VOR ORT
ODER ONLINE MÖGLICH

u. a. mit diesen Themen:

Themenblock 1 Cyberangriffe:

- **Cyberangriff zum Nachverfolgen: Live-Hack**
Svenja Mischur, Managing Consultant IT-Forensik, Master of Engineering IT-Sicherheit und Forensik, Kriminalkommissarin, intersoft consulting services AG
- **Cybercrime und der Paradigmenwechsel in der Strafverfolgung – Was können Strafverfolger leisten und wie gelingt die Zusammenarbeit mit betroffenen Unternehmen?**
Jana Ringwald, Oberstaatsanwältin, Generalstaatsanwaltschaft Frankfurt am Main – ZIT
- **Zwischen allen Fronten?**
Die Rolle des Compliance Officers beim Cyberangriff – Austausch mit Behörden, CISO und dem DSB
Dr. Dietmar Deffert, Regional Chief Compliance & Security Officer Europe, Schaeffler Group

Themenblock 2 Hinweisgeber

- **Die Perspektive des Hinweisgebers – Ein Erfahrungsbericht**
Annegret Falter, Vorsitzende, Whistleblower Netzwerk e.V.
- **Zum Nutzen von Ombudspersonen in Zeiten der EU-Hinweisgeberrichtlinie**
Anika Feger, Rechtsanwältin & Ombudsperson, Compliance Law Office – Feger Rechtsanwälte
- **Ein Hinweis geht ein... Was ist zu tun? Wie die Compliance-Abteilung mit Hinweisen umgeht**
Caroline Schüller, ehem. Staatsanwältin, Compliance Manager, ADAC Compliance Service GmbH und Karolina Trispel, LL.M., Compliance Manager, ADAC Compliance Service GmbH

Themenblock 3 Lieferkette

- **Aktuelle Rechtsfragen bei LkSG und ESG**
Dr. Malte Passarge, Partner, HUTH DIETRICH HAHN Rechtsanwälte
- **LkSG – Wohin muss Compliance schauen?**
Elke Wurster, Head of Compliance, TÜV SÜD AG
- **Internationale Compliance-Anforderungen digital und nachhaltig meistern**
Dominik Nowak, Managing Director & Legal Representative China, Martin Mantz GmbH

... und viele mehr!

Maria Belz

dfv Mediengruppe, Mainzer Landstr. 251, 60326 Frankfurt a.M.
Tel.: +49 69 7595-1157 | Fax: +49 69 7595-1150 | maria.belz@dfv.de



Bescheinigung von 10 Stunden und
15 Minuten für Ihre berufliche Weiterbildung.



Melden Sie sich jetzt an!

www.deutsche-compliance-konferenz.de

Mit freundlicher Unterstützung von:



Medienpartner:



Neobanken – Regelungslücke im Aufsichtsrecht?

Die Bedeutung sogenannter Neobanken auf dem Bankenmarkt nimmt stetig zu. Die Geschäftsmodelle sowie die rechtlichen Konstrukte dieser unter dem Titel Neobanken, aber auch Challenge-Banken, Online-Banken, Internet-only-Banken, virtuelle oder digitale Banken geführten Institute stellen die Aufsicht vor Herausforderungen. Dies beeinträchtigt nicht nur die Interessen der Verbraucher und deren Vertrauen in einen ordnungsgemäß funktionierenden Finanzdienstleistungsmarkt. Eine aufsichtsrechtliche Sonderbehandlung dieser „neuen“ Erscheinungsform von Banken, Kreditinstituten und Finanzdienstleistern könnte darüber hinaus diesen – im Vergleich zu den bestehenden „Präsenz-“, oder „Real-“ Banken – einen ungerechten wettbewerblichen und unternehmerischen Vorteil vermitteln.



Neobanken bieten ihre Leistungen ausschließlich im Internet an und haben darum kein eigenes Vertriebsstandort- oder Filialnetz.

Neobanken sind Finanztechnologie-Unternehmen (FinTechs), die – im Gegensatz zu den klassischen Bank-, Kredit- bzw. Finanzdienstleistungsinstituten – ihre Leistungen ausschließlich digital, d.h. im Internet, anbieten und somit über kein eigenes physisches Vertriebsstandort- oder Filialnetz verfügen. Die Loslösung ihrer Geschäftstätigkeit verschafft Neobanken einen unbestreitbaren wirtschaftlichen Vorteil gegenüber den klassisch tätigen Instituten. Diese Vorteile können Neobanken in Gestalt von niedrigen Gebühren weitergeben. Allerdings müssen Kunden bei dieser Form des Bankings ausdrücklich auf ihre persönliche Beratung verzichten.

Grundsätzliche Probleme schafft die Zuordnung von Neobanken und deren Geschäften zum Anwendungsbereich des Gesetzes über den Wertpapierhandel (WpHG) oder des Gesetzes über das Kreditwesen (KWG) bzw. des sie konkretisierenden MaComp bzw. der MaRisk. Ohnehin ist fraglich, ob, und wenn ja, wie Neobanken dem derzeitigen Banken- und Finanzdienstleistungsaufsichtsrecht unterliegen. Als aufsichtsbehördliches Eingriffsrecht bedarf dieses Recht einer speziellen Ermächtigung um nicht allzu großzügig auf alle möglichen Erscheinungsformen im Bank- und Kapitalmarktrecht ungehindert Anwendung finden zu können.

Das Bankenaufsichtsrecht kommt bei Neobanken immer dann zur Anwendung, wenn Bank-, Kredit- bzw. Finanzdienstleistungsinstitute in Gefahr stehen durch ihre Geschäftshandlungen Ziele der Aufsicht zu konterkarieren. Damit kommt es

entscheidend auf die Handlungen, bzw. die Handlungspflichten der Institute, und zweitens auf das Risiko an, das Institute – unabhängig von ihrer Bezeichnung – auf den Banken- und Kapitalmarkt realisieren.

Um diese Frage eingehend beantworten zu können, ist zwischen den derzeit drei existenten Typen von Neobanken und deren Risiken zu unterscheiden:

1. Neobanken mit Vollbanklizenz: Diese Neobanken unterscheiden sich in ihrer aufsichtsrechtlichen Ausprägung nicht von den klassischen Kreditinstituten im Sinne des § 1 Abs. 1 KWG oder der Kapitaladäquanzverordnung (CRR). Die Neobanken mit Vollbanklizenz sind vollständig reguliert und unterliegen somit der vollständigen Aufsicht. Vor Herausforderungen stellt die Aufsicht insbesondere die Bewertung der kontinuierlich neu entstehenden Geschäftsmodelle.

2. Neobanken als vertraglich gebundene Vermittler: Sie verfügen selbst über keine Vollbanklizenz, werden jedoch als vertraglich gebundener Vermittler im gleichnamigen Register der BaFin geführt. Ein haftendes Institut stellt für vertraglich gebundene Vermittler ein Haftungsdach sowie in der Regel auch die Abwicklungsinfrastruktur für die vermittelten Geschäfte zur Verfügung. Der vertraglich gebundene Vermittler tritt gegenüber dem Kunden mit eigener Marke auf. Die Geschäftsabwicklung

erfolgt jedoch auf Namen und auf Rechnung des haftenden Instituts. Die vertraglich gebundenen Vermittler i. S. d. § 2 Abs. 10 KWG bzw. § 3 Abs. 2 WpHG benötigen für die Ausübung ihrer Tätigkeit keine Erlaubnis. Darüber hinaus finden die Bestimmungen des Geldwäschegesetzes (GwG) i. d. R. keine Anwendung, da der vertraglich gebundene Vermittler meist unter die Ausnahmeregelung des § 2 Abs. 10 KWG fällt und so kein „Verpflichteter“ i. S. d. § 2 Abs. 1 Nr. 2 GwG ist.

3. Neobanken als reine Anbieter („Banking-Frontend“): Neobanken als reine Banking-Anbieter nutzen sog. Banking-as-a-Service- oder White-Label-Banking-Lösungen. Hierbei stellt ein (CRR-)Kreditinstitut i. S. d. § 1 Abs. 1 bzw. Abs. 4 KWG seine Infrastruktur zur Verfügung und vertreibt Banking-Produkte unter der Marke der Neobank. Das (CRR-)Kreditinstitut lagert alle Marketing- und Vertriebsaktivitäten an eine Neobank aus und bezieht formell auch das Banking-Frontend von dieser. Aus Perspektive des Kunden erfolgt ein Login über die App oder den Internetauftritt der Neobank. Diese Auftritte sind jedoch lediglich eine Benutzeroberfläche, die komplette technische Infrastruktur im Hintergrund wird vom (CRR-)Kreditinstitut bereitgestellt. Vertragspartner des Kunden ist das (CRR-)Kreditinstitut. Sofern die Neobank keinen Zugriff auf die Daten des Kunden hat und diese nur durchleitet, gehen die Risiken für den Finanzmarkt sowie den Kunden lediglich vom (CRR-)Kreditinstitut aus. Die Beaufsichtigung richtet sich an das (CRR-)Kreditinstitut. Die Neobank wird jedoch mittelbar beaufsichtigt, da das (CRR-)Kreditinstitut Risikoanalysen durchführen muss und dafür Sorge trägt, dass die Auslagerung im Sinne der ordnungsgemäßen Geschäftsorganisation erfolgt.

Die Quantität und Diversität der Institute erschweren die rechtliche Beurteilung. Verschiedene Regelungslücken, gerade auch im Aufsichtsrecht, sind die Folge. Prof. Dr. jur. Dieter Krimphove und René Knoblich



Prof. Dr. jur. Dieter Krimphove ist Jean Monnet-Professor „ad personam“ und Inhaber des Lehrstuhls für Wirtschaftsrecht und Europäisches Wirtschaftsrecht an der Universität Paderborn sowie Gastprofessor an der Donau-Universität Krems und an der Universität Strasbourg.



René Knoblich ist Manager bei BearingPoint im Bereich Banking & Capital Markets. Schwerpunkt seiner Arbeit sind technisch gestützte Compliance-Lösungen für den Banken- und FinTech-Markt. Er ist Co-Autor im MaRisk-Kommentar aus der Reihe „Gelbe Erläuterungsbücher“.

Mehr zum Thema und insbesondere zur aufsichtsrechtlichen Einordnung sogenannter „Neobanken“ lesen Sie in der Juli-Ausgabe des **Compliance-Beraters**, die am 30. Juni 2022 erscheint.



11.-12. Oktober 2022

EUROPEAN COMPLIANCE AND ETHICS CONFERENCE

Bei Europas größter Konferenz für Ethik- und Compliance-Themen erwarten Sie zwei volle Tage mit Keynotes, Interviews, Podiumsdiskussionen, Workshops und Breakout-Sessions mit inspirierenden Rednern und führenden Ethik- und Compliance-Experten. **Die ECEC 2022 findet als hybrides Event statt.**



Vor Ort in München



Virtuell



5.000+

Teilnehmende



70+

Speaker



40+

Sessions &
Keynotes

Jetzt anmelden!

www.ecec-community.com

Online-Anbieter müssen nicht immer über Herstellergarantien informieren

Im Streit darum, ob Online-Anbieter Informationen zu Herstellergarantien bereitstellen müssen, hat der EuGH nun ausgleichend geurteilt. Diese Informationspflicht bestehe nur dann, wenn der Verbraucher ein berechtigtes Interesse daran habe – etwa, wenn die Herstellergarantie als Werbe- und Verkaufsargument eingesetzt wird.



Online-Anbieter: Wer die Herstellergarantie als Verkaufsargument einsetzt, muss auch über sie informieren.

Am 5. Mai 2022 hat der **EuGH (C-179/21)** über die Frage geurteilt, ob ein Online-Anbieter verpflichtet ist, den Verbraucher über das Bestehen einer gewerblichen Garantie des Herstellers zu informieren. Im konkreten Fall wollte ein Anbieter von Taschenmessern ein gerichtliches Verbot erwirken, damit ein Konkurrent künftig ein Produkt nicht mit Herstellergarantien bewirbt, ohne hierbei auf die gesetzlichen Regelungen zu Garantien hinzuweisen.

Der BGH, vor dem das Verfahren zunächst verhandelt wurde, hatte den Streit dem EuGH vorgelegt. Der EuGH stellte fest, dass die Pflicht, den Verbraucher über das Bestehen einer gewerblichen Garantie des Herstellers zu informieren, sämtliche für diese Ware bedeutsamen Informationen abdeckt. Der Verbraucher müsse anhand dieser Informationen entscheiden können, ob er sich vertraglich an den Unternehmer binden möchte. Diese Informationen umfassen

die wesentlichen Eigenschaften der Waren sowie grundsätzlich alle untrennbar mit der Ware verbundenen Garantien, darunter die vom Hersteller angebotene gewerbliche Garantie. Der EuGH weist allerdings darauf hin, dass die Übermittlung von Informationen über die gewerbliche Garantie des Herstellers zwar ein hohes Schutzniveau für den Verbraucher sicherstellt, eine unbedingte Verpflichtung, solche Informationen stets zur Verfügung zu stellen, aber unverhältnismäßig erscheint. Im Rahmen der Abwägung zwischen einem hohen Verbraucherschutzniveau und der Wettbewerbsfähigkeit der Unternehmen kommt das Gericht zu dem Befund, dass der Online-Anbieter nur dann verpflichtet ist, dem Verbraucher vorvertragliche Informationen über eine gewerbliche Garantie des Herstellers zur Verfügung zu stellen, wenn der Verbraucher ein berechtigtes Interesse am Erhalt dieser Informationen hat, um die Entscheidung zu treffen, ob er sich vertraglich an den Unternehmer binden möchte. Dieses Interesse liege vor, wenn der Unternehmer die gewerbliche Garantie des Herstellers zu einem zentralen oder entscheidenden Merkmal seines Angebots macht. Das sei insbesondere dann der Fall, wenn er daraus ein Verkaufs- oder Werbeargument herleitet, um die Wettbewerbsfähigkeit oder die Attraktivität seines Angebots im Vergleich zu den Angeboten seiner Wettbewerber zu verbessern.

Für Philipp Rohdenburg, Rechtsanwalt bei CMS Deutschland, ist dieses Urteil „etwas überraschend“. Denn entgegen seiner oftmals verbraucherfreundlichen Linie habe der EuGH hier zumindest teilweise zugunsten der Online-Händler entschieden.

Zwar entstehe für Online-Händler ein Mehraufwand, da diese sich damit auseinandersetzen müssen, ob die Hersteller der von ihnen vertriebenen Produkte die Herstellergarantie als Verkaufs- oder Werbeargument einsetzen. Eine allgemeine Informationspflicht, die kaum überwindbare Hürden für Händler geschaffen hätte, gerade wenn sie nichteuropäische Produkte anbieten, bestehe jedoch nicht.

„Für Verbraucher bedeutet die Entscheidung mehr Transparenz im Onlinehandel, während der für Händler entstehende Mehraufwand im Rahmen der Angebotsgestaltung in den meisten Fällen noch darstellbar sein dürfte“, ordnet Rohdenburg ein.

Das habe auch für den deutschen Markt und insbesondere für deutsche Online-Anbieter unmittelbare Folgen: „Wird ein Angebot mit einer Garantie beworben, muss der Anbieter sämtliche Informationen hinsichtlich der Garantie bereitstellen. Andernfalls riskiert er eine Abmahnung.“ *chk*

IMPRESSUM

Verlag

Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
UStIdNr. 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: Eva Triantafyllidou,
Telefon: 069 7595-2713, E-Mail: Eva.Triantafyllidou@dfv.de

Mitherausgeber:

BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH

Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe AG; 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 Leffrag, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Corpus Sireo Holding GmbH; 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

Jede Verwertung innerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Keine Haftung für unverlangt eingesandte Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeicherung in eine Datenbank.

© 2022 Deutscher Fachverlag GmbH, Frankfurt am Main

Deutsche
Compliance Konferenz 2022

28. & 29. Juni 2022, Frankfurt am Main
Cyberangriffe • Hinweisgeber • Lieferkette

HYBRID:
TEILNAHME
VOR ORT ODER
ONLINE

juris

KANN ICH DAS RISIKO VON GELDWÄSCHE MINIMIEREN? **JA. MIT JURIS.**

Geldwäscheprävention spielt für Unternehmen eine zentrale Rolle, um rechtliche und wirtschaftliche Konsequenzen sowie Imageschäden auszuschließen. Die Komplexität der Bestimmungen und die hohe Änderungsdynamik birgt die Gefahr, dass veraltete Regelungen zur Anwendung kommen oder Wichtiges übersehen wird. Mit juris Geldwäsche Praxis erhalten Sie erstmals eine praxisorientierte Komplettlösung, die Ihnen an einem Ort alles bietet, um Freigabeprozesse schnell und rechtlich zuverlässig durchzuführen.



Jetzt hier gratis testen.



juris.de Wissen, das für Sie arbeitet.

BaFin: „Finanzstabilität ist kein Selbstläufer“

Zur Jahrespressekonferenz der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) am 3. Mai 2022 stellte ihr Präsident, Mark Branson, insbesondere die Risiken für das deutsche Finanzsystem und dessen Stabilität heraus. Der Krieg in der Ukraine habe ins Gedächtnis gerufen, dass Finanzstabilität kein Selbstläufer ist.



Marc Branson, Präsident der BaFin, betonte zur Jahrespressekonferenz der Behörde insbesondere Risiken, die infolge des Kriegs in der Ukraine für die Finanzbranche bestehen.

Die direkten Auswirkungen des Kriegs und der gegen Russland und Belarus verhängten Sanktionen dürften – Stand jetzt – für das deutsche Finanzsystem verkräftbar sein“, schätzte Branson die Lage ein. Die unmittelbaren Verflechtungen mit diesen Ländern und der Ukraine seien begrenzt.

Problematisch könnten allerdings die schwer einschätzbaren Zweit- und Drittrundeneffekte werden, warnte der BaFin-Präsident. Der Krieg bremse weltweit das Wirtschaftswachstum, störe Handelsbeziehungen, treibe die Preise von Gas, Öl und anderen Rohstoffen in die Höhe und verschärfe das Problem der Lieferengpässe. Infolgedessen steige die Inflation, was Zinsanhebungen immer wahrscheinlicher mache, auch in der Eurozone. „Und wir wissen, dass die militärische, handelspolitische oder energiepolitische Lage jederzeit stark eskalieren könnte, woraufhin es unweigerlich zu Markturbulenzen käme“, so Branson. Die Finanzaufsicht müsse risikoorientiert agieren und versuchen, im Vorhinein zu erkennen, an welchen Stellen und unter welchen Bedingungen das Finanzsystem besonders verwundbar ist.

Das seit langem niedrige Zinsniveau sei nach wie vor eine der größten Herausforderungen für

die deutsche Finanzbranche. Das Dauerzinstief habe auch den deutschen Banken, Sparkassen und Bausparkassen zugesetzt, denn der Zinsüberschuss mache traditionell einen wesentlichen Teil ihrer Erträge aus. Hinzu komme das inflationsbedingt wachsende Zinsänderungsrisiko: Ein abrupter und kräftiger Zinsanstieg könne die Banken in Schwierigkeiten bringen. Ihre kurzfristig angelegten Refinanzierungen würden plötzlich teurer, während ihre Zinseinkünfte aufgrund langer Zinsbindungen langsamer stiegen. Welche deutschen Banken in diesem Szenario besonders gefordert wären, prüfe die BaFin gerade. Gemeinsam mit der Deutschen Bundesbank unterzieht die BaFin seit Anfang April Institute, die unter ihrer direkten Aufsicht stehen einem Stresstest und spielt dabei verschiedene Zinsszenarien durch.

Der wirtschaftliche Abschwung durch den Krieg und zuvor durch Corona ist ein zusätzliches Problem, das ein steigendes Risiko für Kreditausfälle mit sich bringe. Die BaFin sehe sich weiterhin die Kreditrisiken von Banken und Sparkassen sehr genau an. Diesmal aber mit Blick auf die energieintensiven oder rohstoffabhängigen Sektoren.

Die Verschuldung von Unternehmen, so Branson, sei in den vergangenen Jahren gestiegen

– vor allem die über komplexe Produkte des Kapitalmarkts. Auf diese Weise seien Kreditrisiken in intransparenten Segmenten des Finanzsystems gelandet, die wenig bis gar nicht reguliert sind. Dass Banken hieran bislang weniger direkt beteiligt seien, sei auch der Re-Regulierung nach der Finanzkrise 2007/2008 zu verdanken. Und doch gebe es Schnittstellen zwischen dem regulierten Bankensektor und dem „non-banking financial institution“ (NBFI)-Sektor.

An dieser „Schnittstelle mit der Welt der Schatzenbanken“ gehe die BaFin konsequent gegen Konzentrationsrisiken vor.

Sehr groß und sehr präsent sei zudem die Gefahr, dass Unternehmen des Finanzsektors Opfer von Cyberangriffen werden oder dass es dort zu internen IT-Sicherheitsvorfällen komme. Solche Vorfälle könnten im Extremfall der Stabilität des Finanzsystems schaden. Niemand wisse, ob Deutschland wirklich auf einen schwerwiegenden Sicherheitsvorfall vorbereitet sei, räumte Branson ein. Der Krieg habe indes Cyberangriffe auch auf den deutschen Finanzsektor wahrscheinlicher gemacht. Seit Kriegsbeginn analysieren die Finanzaufsichter täglich unter anderem die Informationen aus dem nationalen Cyber-Abwehrzentrum und informieren die Finanzindustrie über mögliche Angriffsmuster. „Und wir nehmen weiterhin dezidierte IT-Prüfungen bei den Instituten und Unternehmen vor“, sagte Branson.

Ein weiteres Risiko sei das der Geldwäsche. Die finanziellen Folgen und die Reputationsschäden für Unternehmen könnten immens sein, „wenn nicht gar existenzgefährdend“, warnte Branson. Ihm sei bewusst, dass die BaFin hier eine sehr hohe Verantwortung trage. „Wir sind daher gerade dabei, die Abteilung Geldwäscheprevention personell zu stärken. Wir wollen mehr Ressourcen in die operative Geldwäscheaufsicht stecken und die Unternehmen besonders eng beaufsichtigen, bei denen wir die größten Probleme sehen. Wo nötig, werden wir eingreifen.“

chk

Neue Grundsätze der Zusammenarbeit

Das Bundesministerium der Finanzen (BMF) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hatten sich 2021 darauf verständigt, die bisherigen „Grundsätze für die Ausübung der Rechts- und Fachaufsicht des BMF über die BaFin“ grundlegend zu überarbeiten. Mitte Mai 2022 legten sie nun die neuen Grundsätze vor.

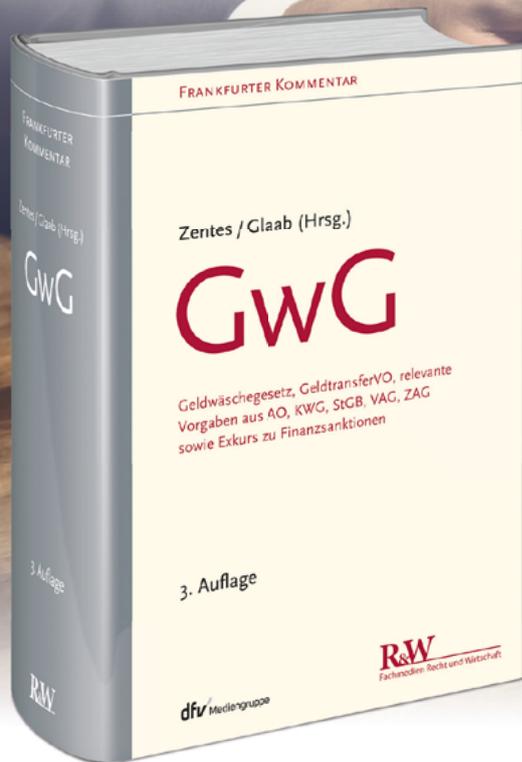
Außer einer stärkeren Verankerung der opera-

tiven Unabhängigkeit der BaFin und der engen Zusammenarbeit zwischen BMF und BaFin in der nationalen, europäischen und internationalen Regulierung werde auch die Rechts- und Fachaufsicht des Ministeriums neu ausgerichtet, teilten BMF und BaFin mit. Die BaFin berichte an das BMF über kritische Entwicklungen bei wichtigen beaufsichtigten Unternehmen oder bei Relevanz für die

Stabilität des Finanzmarkts, eines Sektors oder beispielsweise bei drohendem erheblichem Schaden für Anleger oder Verbraucher. Dies ermögliche es dem BMF, die Erfüllung des gesetzlichen Aufsichtsmandats zu überprüfen. Gleichzeitig bleibe die Eigenverantwortung der BaFin bei der Einzelaufsicht gewahrt. Die neuen Grundsätze der Zusammenarbeit zwischen BMF und BaFin sind [hier abrufbar](#).

Neuaufgabe

Geldwäschegesetz auf aktuellem Stand



Branchenübergreifender Praktiker-Kommentar

Die Autoren kommentieren praxisorientiert für alle tangierten Branchen die gesetzlichen und regulatorischen Vorgaben zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung im deutschen Recht. Ergänzend werden wesentliche Grundlagen für den Umgang mit Finanzsanktionen dargestellt. Die Kommentierung richtet sich in erster Linie an Personen, die täglich mit der Einhaltung und Umsetzung der Vorgaben beschäftigt sind.

Die Neuaufgabe berücksichtigt

- Sämtliche Auslegungs- und Anwendungshinweise zum GWG
- Rundschreiben der Aufsichtsbehörden, Guidelines der EBA
- Sämtliche aktuellen EU-Richtlinien und relevanten Umsetzungsgesetze, wie insbesondere
 - Gesetz zur strafrechtlichen Bekämpfung der Geldwäsche, Finanzmarktintegritätsstärkungsgesetz (FISG), Transparenzregister- und Finanzinformationsgesetz (TraFinG) und das Gesetzgebungspaket der EU zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung
- Aktuelle deutsche und europäische Gesetzesvorhaben
- Exkurs: Finanzsanktionen und deren grundlegende Betrachtungen sowie praxisrelevante Fragestellungen

Die Herausgeber

Dr. **Uta Zentes**, LL.M. ist Rechtsanwältin und Leiterin Compliance im Finanzsektor. Zuvor hatte sie über mehrere Jahre verschiedene Leitungspositionen in der Compliance-Funktion einer Großbank inne. Außerdem war sie viele Jahre in Big Four-Gesellschaften in der Beratung und Prüfung von Compliance-Themen tätig. Frau Dr. Zentes ist Autorin zahlreicher Fachartikel zum Thema Geldwäscheprävention und Compliance.

Sebastian Glaab ist selbständiger Rechtsanwalt. Zuvor war er mehrere Jahre als Berater bei einer Prüfungsgesellschaft tätig. Er ist Autor zahlreicher Fachbeiträge zum Thema Geldwäscheprävention und Compliance.

Zentes/Glaab (Hrsg.)

GWG – Geldwäschegesetz, GeldtransferVO, relevante Vorgaben aus AO, KWG, StGB, VAG, ZAG sowie Exkurs zu Finanzsanktionen

3., aktualisierte und erweiterte Auflage 2022 | Frankfurter Kommentar | vorbestellbar | ca. 1.500 Seiten | geb. | ca. € 269,- | ISBN: 978-3-8005-1808-1

Weitere Informationen

shop.ruw.de/18081

Keine Buch-Neuerscheinung mehr verpassen? Abonnieren Sie doch gerne unseren Newsletter: shop.ruw.de/newsletter

Hinweisgebersystem im Mittelstand: so viel wie nötig, so wenig wie möglich

Am 13.4.2022 hat das Bundesministerium für Justiz und Verbraucherschutz (BMJV) den lang erwarteten Entwurf für ein Hinweisgeberschutzgesetz (HinSchG-E) vorgelegt. Mittelständische Unternehmen sind stets bestrebt, überbordende Administration zu vermeiden und betrachten zu Recht den Kosten-Nutzen-Aspekt von Regelungen und Anforderungen kritisch. Bevor nun also eine weitere regulatorische Bürde aus Brüssel beklagt wird und moralische Bedenken („Denunziantentum!“) geäußert werden, lohnt es sich, die Vorteile eines Hinweisgebersystems zu betrachten.

Methode/ Prozess	Briefkasten	„Hotline“	E-Mail -Postfach	Ombudsperson	Digitales Hinweisgebersystem (online Meldung)
Verfügbarkeit 24/7/365	✓	✓	✓	(✓)	✓
Anonymität möglich	✗	✓	(✓)	✓	✓
Datensicher	✗	✗	✗	✓	✓
Revisionsicher	✗	✗	✗	(✓)	✓
Sprachenvielfalt	✓	✓	✓	(✓)	✓
2-Wege Kommunikation	(✓)	(✓)	✓	✓	✓
Erhöhter technischer/organisatorischer Aufwand	✗	✗	✗	(✓)	✓
Niedrigschwellig	✓	✓	✓	(✓)	✓
Kosten	niedrig	niedrig	niedrig	mittel	mittel - hoch

Übersicht über verschiedene Hinweisgebersysteme

Das HinSchG-E verpflichtet Unternehmen mit mehr als 50 Beschäftigten, Meldekanäle für Personen, die „im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über (Gesetzes-)Verstöße“ melden wollen, einzurichten. Die Verpflichtung kann auch Unternehmen mit weniger Mitarbeitenden treffen, wenn das Unternehmen in einem „Hochrisikobereich“ tätig ist, wie z.B. Wertpapierdienstleistungsunternehmen, Datenbereitstellungsgesellschaften und ähnliche, regulierte Unternehmen. Unternehmen mit bis zu 249 Mitarbeitenden haben gem. § 42 HinSchG-E bis zum 17.12.2023 Zeit, die Anforderungen des HinSchG-E umzusetzen.

Häufig sind es gerade sehr lokale Mitarbeitende, die ihr Unternehmen vor Schaden schützen wollen und zugleich Konflikte erleben, die sie daran hindern, ihre Meldung offen im Unternehmen kundzutun. In solchen Fällen ist das Hinweisgebersystem ein überaus „wert“-volles Frühwarnsystem. Zu-

gleich kann die Einrichtung eines unternehmenseigenen Hinweisgebersystems verhindern, dass die meldende Person sich direkt an externe Meldestellen oder die Öffentlichkeit wendet. Bei einer Meldung über gut bekannte interne Meldekanäle hat das Unternehmen die Möglichkeit, zunächst ohne Polizei und Behörden eine interne Sachverhaltsaufklärung zu betreiben. So kann es selbst Missstände beheben oder, wenn es z.B. rechtlich geboten ist, Kontakt mit Behörden aufnehmen. Gegebenenfalls kommen sogenannte Selbstanzeigen oder weitere strafmildernde oder sogar strafausschließende Handlungen in Betracht.

Leider gibt das HinSchG-E nicht der Meldung über interne Kanäle den Vorzug. Das Unternehmen kann aber sicher bei der Gestaltung der Information an die Mitarbeitenden zum Hinweisgebersystem und den externen Meldemöglichkeiten die Vorteile der internen Meldung herausstreichen.

Da Ziel des HinSchG-E der Schutz der hinweisgebenden Person ist, und damit die Vertraulichkeit der

Identität derselben in jedem Fall zu gewährleisten ist, stellt sich nun die Frage nach einer für das mittelständische Unternehmen angemessenen und ausreichenden Lösung.

Der Briefkasten ist dabei wohl eher nicht die Lösung, die diesen Anforderungen genügt. Mitarbeitende, die eine Meldung abgeben wollen, können bei Einwurf einer Meldung in den Briefkasten gesehen werden. Jeder kann theoretisch die Nachricht herausfischen, sie vernichten – und bei einer anonymen Meldung ist eine Rückfrage bei der meldenden Person und damit auch die rechtlich zwingende Empfangsbestätigung unmöglich.

Bei Einrichtung einer internen E-Mail-Adresse hingegen ist die

rechtlich geforderte Empfangsbestätigung möglich. Allerdings weiß der Hinweisgebende nicht sicher – wie auch im Fall des Briefkastens –, bei wem die E-Mail am Ende landet. Das schwächt das Vertrauen in eine solche Lösung. Darüber hinaus ist die Datensicherheit – und damit Vertraulichkeit – bei einer internen E-Mail nicht zwingend gewährleistet, denn die interne IT-Administration hat nicht nur theoretisch Zugriffsmöglichkeiten.

Ähnliches gilt für eine sogenannte Hotline, also im einfachsten Fall eine unternehmensinterne Telefonnummer mit Anrufbeantworter, oder die Beantwortung von Anrufen durch ein Callcenter. Bei einem Anrufbeantworter ist wiederum nicht klar, wer den Anruf abhören kann; damit wäre die Vertraulichkeit gefährdet.

Vor diesem Hintergrund erscheint ein extern installiertes, online verfügbares Meldesystem die deutlich bessere Lösung. Hier sind mittlerweile auf dem Markt eine Vielzahl von Anbietern zu finden. Insbesondere für Unternehmen mit ausländischen Tochtergesellschaften kann dies eine gute Lösung für Nachrichten in Textform und die weitere Bearbeitung der Meldung sein.

Erfreulicherweise sieht § 14 Abs. 2 HinSchG-E – anders als eine Mitteilung des Expertenrates der Europäischen Union es angekündigt hat – derzeit die Möglichkeit vor, dass sich mehrere Unternehmen mit 50 bis 249 Beschäftigten eine gemeinsame Meldestelle einrichten können, wobei es für jedes Unternehmen separate Zugänge geben muss. Hier ist dann möglicherweise Raum für Lösungen auf Wirtschafts- oder Interessenverbandsebene.

Schließlich gibt es noch die Möglichkeit eines Meldesystems über eine Ombudsperson. Diese kann sowohl intern als auch extern angesiedelt sein.

Pia Windoffer, LL.M.



Pia Windoffer, LL.M., ist als Of Counsel für die Rechtsanwaltskanzlei Deloitte Legal Rechtsanwalts-gesellschaft mbH tätig. Zuvor war sie ca. 20 Jahre in verschiedenen Unternehmen inhouse überwiegend in leitender Funktion für Integrität und Compliance tätig.

ANMELDUNG >>> www.compliance-academia.de/9vcic

DICO-
Standards

Compliance
Defence im
Kartellrecht

Lieferketten
Compliance
Management

DCGK-
Reform

Auf dem Weg
zum
gemeinsamen
Compliance-
Verständnis?!

Standards &
Zertifizierung:
ISO 37301,
PS 980,
DICO?

HinSchG-
Entwurf

9

. VIADRINA COMPLIANCE & INTEGRITY CONGRESS

21.-22.06.2022 | 40 REFERENT*INNEN | 9 THEMEN | ONLINE

VERANSTALTER



PARTNER & SPONSOREN



EuG bestätigt EZB-Beschluss: Keine Bank-Beteiligung für Berlusconi

Aufgrund seiner Verurteilung wegen Steuerbetrugs im Jahr 2013 erfülle Silvio Berlusconi nicht die für Inhaber von qualifizierten Beteiligungen geltende Anforderung an den Leumund, beschied das Gericht der Europäischen Union (EuG) Mitte Mai und untersagte damit dem ehemaligen italienischen Ministerpräsidenten den Erwerb einer qualifizierten Beteiligung an Banca Mediolanum.

Im Jahr 2015 wurde die Finanzholdinggesellschaft Mediolanum auf ihre Tochtergesellschaft Banca Mediolanum verschmolzen. Angesichts ihrer Beteiligung am Gesellschaftskapital von Mediolanum wurde Fininvest, eine mehrheitlich von Silvio Berlusconi gehaltene Holdinggesellschaft italienischen Rechts, Inhaberin einer Beteiligung am Kapital von Banca Mediolanum.

Zuvor hatte die Banca d'Italia (italienische Zentralbank) unter anderem entschieden, den Antrag auf Genehmigung einer qualifizierten Beteiligung an der Banca Mediolanum mit der Begründung abzulehnen, dass Berlusconi aufgrund seiner Verurteilung wegen Steuerbetrugs im Jahr 2013 die

Anforderung an den Leumund nicht mehr erfülle. Diese Entscheidung der italienischen Zentralbank wurde durch ein Urteil des Consiglio di Stato (Staatsrat Italien) vom 3. März 2016 aufgehoben.

Nach der Verschmelzung von Mediolanum und Banca Mediolanum sowie dem Urteil des Staatsrats vom 3. März 2016 eröffneten die italienische Zentralbank und die Europäische Zentralbank (EZB) ein neues Verfahren zur Beurteilung des Erwerbs einer qualifizierten Beteiligung an Banca Mediolanum. Nach Abschluss dieses Verfahrens erließ die EZB einen Beschluss, mit dem sie die Genehmigung des Erwerbs einer qualifizierten Beteiligung an diesem Kreditinstitut versagte. Die



Bekannt für Skandale: Silvio Berlusconi, ehemaliger italienischer Staatspräsident und Unternehmer.

EZB begründete dies insbesondere damit, dass Berlusconi die für Inhaber von qualifizierten Beteiligungen geltende Anforderung an den Leumund nicht erfülle.

Das EuG teilt diese Auffassung und trifft in seinem Urteil wichtige Klarstellungen zum Erwerb einer qualifizierten Beteiligung an einem Kreditinstitut durch eine Person, die das Leumundskriterium nicht erfüllt. Das Gericht stellt in diesem Zusammenhang unter anderem klar, dass der Leumund des interessierten Erwerbers nicht vom Ausmaß seines voraussichtlichen Einflusses auf das Kreditinstitut abhängig ist.

chk

Deutsche Compliance Konferenz 2022: ein Ausblick

Cyberangriffe, Hinweisgeber, Lieferkette – diese drei aktuellen Themen der Compliance-Community stehen im Mittelpunkt der Deutschen Compliance Konferenz am 28. und 29. Juni 2022.

Durch die Tagung führen erneut als bewährtes Moderatoren-Team Jörg Bielefeld und der Chefredakteur des Compliance-Beraters Dr. Malte Passarge. Zu Beginn der Veranstaltung wird Jörg Bielefeld ein Update zu den Verbandssanktionen und der aktuellen Sicht des Bundesgerichtshofes auf Compliance geben. Anschließend startet die Konferenz in den ersten Themenblock „Cyberangriffe“. Ein Thema das Compliance-Verantwortliche zunehmend unter Druck setzt, denn Deutschland gilt als „lukratives Angriffsziel“ und ist darum besonders stark betroffen. Die Sorge vor einer noch stärkeren Zunahme der Cyberangriffe steigt zudem durch den Krieg in der Ukraine.

Mit vier Fachvorträgen und einer anschließenden Paneldiskussion wird die Thematik von allen Seiten beleuchtet. Einen „Cyberangriff zum Nachverfolgen: Live-Hack“ zeigt Svenja Mischur auf. Was Strafverfolger leisten können und wie die Zusammenarbeit mit betroffenen Unternehmen gelingt, beschreibt im Anschluss Oberstaatsanwältin Jana Ringwald. Mit der Perspektive der Datenschutz-Compliance beschäftigt sich Jana C. Fuchs in ihrem Vortrag „Cyberangriff auf Unternehmens- und Kundendaten: Sind Unternehmen Opfer und Täter zugleich?“ Dr. Dietmar Deffert berichtet über die Rolle des Compliance Officers

beim Cyberangriff und den Austausch mit Behörden, dem Chief Information Security Officer und dem Datenschutzbeauftragten.

Der zweite Konferenztag beginnt mit dem Themenblock „Hinweisgeber“, der durch den erst im April vorgelegten neuen Entwurf zum Hinweisgeberschutzgesetz höchste Aktualität hat. Mit einem kurzen Aufriss zum Thema macht Jörg Bielefeld den Auftakt. Eine für Compliance-Verantwortliche eher ungewohnte Sicht, nämlich die Perspektive des Hinweisgebers, bietet Annegret Falter, Vorsitzende des Whistleblower Netzwerk e.V., in ihrem Erfahrungsbericht. Katrin Hellebrand, EQS Group AG, beschreibt im Anschluss, wie digitale Hinweisgebersysteme im operativen Compliance-Alltag helfen können. Über den Nutzen von Ombudspersonen im Hinweisgeberschutz berichtet Rechtsanwältin Anika Feger. Auch der Datenschutz spielt im Kontext des Whistleblowings eine wichtige Rolle. Christian Nickel LL.M., Compliance Manager bei der DB Netz AG, berichtet in diesem Zusammenhang über „Compliance zwischen Aufklären, Abwehren und Informieren“.

Die ehemalige Staatsanwältin Caroline Schüler und Karolina Trispel, LL.M., beide Compliance Manager bei der ADAC Compliance Service GmbH, stellen dar, wie die Compliance-Abteilung mit Hin-

weisen umgehen sollte: Best-Practice aus Compliance-Perspektive.

Der Konferenz-Nachmittag steht dann anschließend ganz im Zeichen der „Lieferkette“. In die aktuellen Rechtsfragen zum LkSG und ESG führt Dr. Malte Passarge ein. Elke Wurster, Head of Compliance, TÜV Süd AG, befasst sich dann ganz mit dem LkSG und klärt die Frage „Wohin muss Compliance schauen?“ Wie internationale Compliance-Anforderungen digital und nachhaltig gemeistert werden können, beschreibt Dominik Nowak.

Mit einer (selbst-)kritischen Bestandsaufnahme unter dem Motto „Compliance – Alles oder nichts?“ schließen Markus Jüttner und Jörg Bielefeld die Konferenz.

Die Veranstaltung findet als Hybrid-Tagung statt: Den Teilnehmern steht es frei, sich online einzuwählen oder im Steigenberger Frankfurter Hof in Frankfurt am Main persönlich die Referenten und Gäste der Tagung zu treffen.

chk

Compliance-Leser erhalten mit dem Gutscheincode OZCOMPLIANCE im [Ticketshop](#) 10 % Rabatt (gültig bis 16. Juni 2022).

Neuerscheinung

Es ist Zeit für einen Perspektivwechsel!



Zum Inhalt

Auf dem Gebiet der Compliance gibt es inzwischen eine fast unüberschaubare Menge an Literatur und Vorschlägen, wie Unternehmenskriminalität verhindert, Regel- und Gesetzestreue sowie Integrität in Organisationen (angeblich) erfolgreich um- und durchgesetzt werden können.

Dieses Werk weicht vom Üblichen ab, greift das Thema aus einer anderen Perspektive auf und klärt unter anderem die Frage, weshalb Compliance-Schulungen überschätzt werden, wie Unternehmenskriminalität jenseits standardisierter Compliance Systeme wirksam bekämpft werden kann und weshalb man nicht seinen Friseur fragen sollte, ob man einen Haarschnitt benötigt.

Der Autor zeigt mit diesem Werk nicht auf, wie man „gute Compliance“ tätigt, sondern wie man „schlechte Compliance“ vermeidet.

Der Autor

Markus Jüttner ist Rechtsanwalt, Vice President und Head of Group Compliance eines DAX-Konzerns sowie Vorstandsmitglied des Deutschen Instituts für Compliance (DICO e. V.), Lehrbeauftragter am Max-Weber-Institut für Soziologie der Universität Heidelberg, der Hochschule Ludwigshafen und Beirat der Simply Rational GmbH, einer Ausgründung des Max-Planck-Instituts for Human Development.

Markus Jüttner

Die Kunst erfolgreicher Compliance Eine etwas andere Sicht auf wirksames Compliance Management

1. Auflage 2022 | Compliance Berater-Schriftenreihe
vorbestellbar | ca. 200 Seiten | Broschur | € 34,90
ISBN: 978-3-8005-1793-0

Weitere Informationen
shop.ruw.de/17930



Keine Buch-Neuerscheinung mehr verpassen? Abonnieren Sie doch gerne unseren Newsletter: shop.ruw.de/newsletter