

Inhalt



Kampfansage an Doping im Spitzensport

Doping-Skandale bringen den Sport und die Sportlerinnen und Sportler in Verruf.

Damit soll nun bald Schluss sein. Geht es nach der Bundesregierung, soll es bereits ab 2016 ein Anti-Doping-Gesetz geben, das das Eigendoping verbietet und die uneingeschränkte Besitzstrafbarkeit vorsieht. Experten halten den Gesetzesentwurf für nicht gut durchdacht.



Kann es Informationssicherheit geben?

Vor einer Ausspähattacke ist kein Unternehmen sicher, der Schaden pro Jahr liegt im zweistelligen Millionenbereich.



Schöne Bescherung ...

Pflege der guten Geschäftsbeziehungen oder strafbare Korruption: Welche Verhaltensregeln sind einzuhalten?



Credit Suisse:

neue Compliance-Verantwortliche

Lara Warner ist Chief Compliance and Regulatory Affairs Officer der Credit Suisse.

Aufmacher

2 Kampfansage an Doping im Spitzensport

Ein neues Gesetz soll das Ansehen des Sports wieder geraderücken.

Recht

6 Geschenke und Essenseinladungen annehmen ... oder lieber doch nicht?

Compliance-Richtlinien machen den Mitarbeitern die Entscheidung leichter.

Karriere

7 Die Deutsche Bank hat eine personelle Neuordnung beschlossen

Konzernaufbau und Führungsstruktur werden grundlegend geändert.

Praxis

4 Unternehmen müssen ihre sensiblen Daten schützen

Denn Hackern geht es längst nicht mehr um ihre informelle Selbstbestimmung und um das Hacken als solches.

6 Veranstaltungen

7 Personalwechsel

Agricultural Bank of China, Boehringer, Credit Suisse und die SOS-Kinderdörfer haben neue Compliance-Verantwortliche.



Das Ansehen des Sports steht auf dem Spiel.

Kampfansage an Doping im Spitzensport

Kabinett beschließt Entwurf für Anti-Doping-Gesetz

Bestechungsvorwürfe, Doping-Skandale: Der Sport ist nicht nur weltweit, sondern auch in Deutschland immer mehr in Verruf geraten. Dabei verkörpert der Sport positive Werte wie Erhaltung der Gesundheit, Leistungsbereitschaft, Fairness und Teamgeist. Er schafft Vorbilder für junge Menschen und ist durch die Sportlerinnen und Sportler mit ihren Spitzenleistungen zugleich Aushängeschild für Deutschland in der Welt. Daneben ist der Sport auch ein wichtiger Wirtschaftsfaktor. Aber genau hier liegt der Hund begraben.

Manche Spitzenleistung lässt Zweifel laut werden. Beim genauen Hinsehen stellt sich nicht selten heraus, dass Sportlerinnen und Sportler sich durch Doping ungerechtfertigte Vorteile verschaffen. Ihre Vorbildfunktion, aber auch die Integrität des sportlichen Wettbewerbs im Allgemeinen wird damit erschüttert. Von Fairness und Chancengleichheit kann nicht mehr die Rede sein.

Auch die Gefahren für die Sportlerinnen und Sportler ist nicht zu unterschätzen. Zahlreiche Todesfälle in der Vergangenheit und schwere Spätfolgen von systematischem Doping sind Beweis für die gesundheitlichen Gefahren.

Damit soll nun bald Schluss sein. Geht es nach der Bundesregierung, soll es bereits ab 2016 ein

Anti-Doping-Gesetz geben, das das Eigendoping verbietet und die uneingeschränkte Besitzstrafbarkeit vorsieht.

Die Bundesregierung nimmt damit den Kampf auf mit kriminellen Strukturen, die durchaus mit denen im organisierten Rauschgifthandel vergleichbar sind. Der illegale Handel mit Dopingmitteln hat inzwischen eine alarmierende Dimension erreicht. Es haben sich organisierte Vertriebswege und Händlerstrukturen entwickelt, und nicht selten sind Minderjährige die Konsumenten.

Auch bisher hat Deutschland die Hände zwar nicht in den Schoß gelegt. Schließlich ist die Bundesrepublik durch das Internationale Übereinkommen vom 19. Oktober 2005 gegen Doping im Sport und das Übereinkommen vom 16. November 1989 gegen Doping völkervertraglich verpflichtet, Maßnahmen zur Dopingbekämpfung zu ergreifen. Allerdings haben diese Maßnahmen nicht die erforderliche Wirkung gezeigt, und auch die strafrechtlichen Bestimmungen weisen Lücken auf, weil sie in vielen Fällen die dopenden Sportlerinnen und Sportler nicht erfassen.

Das geplante Anti-Doping-Gesetz sieht nun ein ganzes Paket von Maßnahmen vor. Neben

neuen Straftatbeständen soll eine umfassende strafrechtliche Sanktionierung möglich sein, und zwar sowohl gegen die Hintermänner und kriminellen Netzwerke als auch gegen die dopenden Sportlerinnen und Sportler selbst. Die Einführung einer Strafbarkeit von Erwerb und Besitz von Dopingmitteln auch bei geringer Menge ist ebenfalls vorgesehen, sofern Selbstdoping beabsichtigt ist. Geldstrafen und Gefängnisstrafen von bis zu drei Jahren können verhängt werden.

Klingt plausibel. Und trotzdem: Rechtsexperten kritisieren den Gesetzesentwurf als unausgereift, unklar, unbestimmt und unverhältnismäßig. Besonders die Besitzstrafbarkeit ab der ersten Pille stößt auf Kritik. Man solle sich im Gesetz auf das Eigendoping konzentrieren – nicht auf die Besitzstrafbarkeit, lautet ein Gegenvorschlag. Auch der Deutsche Olympische Sportbund (DOSB) hat Bedenken gegen den Straftatbestand des Selbstdopings angemeldet.

Das letzte Wort in dieser Sache ist sicherlich noch nicht gesprochen. Presseberichten zufolge bereiten Innenministerium und Justizministerium bereits die ersten Änderungen am Gesetzesentwurf vor. Das Gesetz soll dann aber zügig – möglichst bis Ende des Jahres – verabschiedet werden. CSZ



cutting through complexity

Einfach. KPMG

Klares Denken, klare Lösungen, klares Handeln: Unsere Experten zeigen nicht nur geschäftliche Chancen auf. Sie helfen, Entwicklungen mitzubestimmen und Wachstumsziele zu erreichen.

Wie können wir Ihre Welt einfacher machen?

Kontakt:

KPMG AG Wirtschaftsprüfungsgesellschaft

Jens Carsten Laue

T +49 211 475-7901

jlaue@kpmg.com

KPMG Rechtsanwaltsgesellschaft mbH

Dr. Konstantin von Busekist

T +49 221 271689-6883

kvonbusekist@kpmg-law.com

www.kpmg.de

News

Lidl führt Online-Compliance-Meldesystem ein

Lidl möchte Fehlverhalten oder Compliance-Verstöße durch oder gegenüber den Mitarbeitern entgegenwirken. Das Unternehmen bietet aber auch die Möglichkeit eines Online-Meldesystems an. Hierfür wurde das Business Keeper Monitoring System eingerichtet. Dabei handelt es sich um eine internetbasierte Anwendung, die von jedem internetfähigen Gerät aus angerufen werden kann.

Info: www.lidl.de/compliance oder www.bkms-system.net/lidl

GEORG: Mit der Compliance-Software zur gerichtsfesten Organisation

Der GEORG Compliance Manager ist eine webbasierte Software zum Nachweis der Einhaltung interner und externer Vorschriften (Compliance). Zu den Tools gehören Legal Management: Gerichtsfeste Organisation der rechtlichen Aufgaben; Genehmigungsmanagement: Sichere Einhaltung aller behördlichen Vorgaben; Einhaltung aller Rechte und Pflichten aus allen Verträgen.

Info: www.martin-mantz.de/

Neu erschienen: Praxiskommentar Public Corporate Governance Kodex

Die Grundsätze zur Corporate Governance im Public Corporate Governance Kodex (PCGK) bilden die Grundlage für eine verantwortungsvolle Führung von Beteiligungen des Bundes an Unternehmen in privater Rechtsform. Bei der Auslegung und Anwendung des PCGK können sich praktische Schwierigkeiten ergeben. Der Praxiskommentar dient als Wegweiser für die zu lösenden Probleme. Von Simone Hartmann € 159,00 inkl. MwSt. ISBN: 978-3-8462-0205-0 2015, 578 Seiten

Ist Informationssicherheit eine Illusion?

Ob Behörden oder Unternehmen: Eine Ausspähattacke jagt die andere, Millionen sicherheitsrelevante Daten werden für dunkle Geschäftsstrategien genutzt, während der Schaden pro Jahr im zweistelligen Millionenbereich liegt. Ist ein Schutz überhaupt möglich, und wenn ja, wie? Wir sprachen dazu mit Stephan Gerhager.

» Die Cyber-Angriffe auf deutsche Unternehmen, Organisationen und Behörden wachsen stetig. Wer verbirgt sich hinter den Angriffen, und welche Motive haben die Angreifer?

« Man kann heute nicht mehr von einer Art Angreifer ausgehen. Auch die Motive der Angreifer haben sich im Laufe der Zeit geändert. In den achtziger

Jahren galten Hacker als Computerfreaks, die sich in fremde Systeme einschleichen konnten, für die jedoch die „Hacker-Ethik“ galt. Es ging nicht um Geld, sondern um Informationsfreiheit. Heute bezeichnet man diese Fraktion der „guten“ Hacker als „White Hat-Hacker“. Für die sogenannten „Black Hats“ hingegen ist Hacken ein Geschäftsmodell. Black Hats spüren Sicherheitslücken auf und verkaufen für hohe, teils sechsstelligen Beträge entweder die Information, wie man in ein System einbrechen kann oder aber die erbeuteten Datensätze.

» Wie gehen diese Black Hats vor?

« Im schwarzen Lager herrscht keinesfalls Homogenität. Man kann zwei Hauptgruppen unterscheiden. Die erste bilden die „Raubritter“. Sie ziehen durch das Netz und nehmen alles mit, was nicht net- und nagelfest ist. Hohen Aufwand scheuen sie. Hat ein Unternehmen seine Daten nicht gut gesichert, greifen die Raubritter an. Sehen die Hacker, dass die Burg über ein ausgeklügeltes Verteidigungssystem verfügt, ziehen sie sofort weiter. Sie vermeiden jeglichen Aufwand. Bietet ein Unternehmen also leichte Beute, steigt automatisch die Chance, Ziel von Cyberkriminellen zu werden.

Die zweite Gruppe geht die Sache weitaus gezielter an. Vor dem Angriff wird ein „Business Case“ erstellt und die Rentabilität geprüft. Welche Daten sind bei einem Unternehmen zu holen? Für welchen Preis kann man sie verkaufen? Wie viel Zeit muss der Angreifer investieren, um an die Daten zu kommen – rechnet sich ein Angriff? Grundsätzlich kann jedes IT-System angegriffen werden. Ob ein Angriff erfolgreich verläuft, ist letztendlich eine



Stephan Gerhager ist Chief Information Security Officer (CISO) der Allianz Deutschland AG.

Frage des Aufwands. Zahlt sich der Aufwand nicht in harter Währung aus, nehmen die Black Hats das nächste Ziel in Angriff.

» Können sich Unternehmen überhaupt schützen, und was empfehlen Sie als CISO?

« Die Herausforderungen für Unternehmen, ihre Systeme und Daten zu schützen, haben sich in den vergangenen Jahren geändert. Früher stand der Begriff „IT-Sicherheit“ im Vordergrund, alles drehte sich um Firewalls und Virens Scanner. Seit einigen Jahren benutzen wir hingegen den Begriff Informationssicherheit. Das bedeutet: Das Unternehmen beschäftigt sich in Form eines aktiven Risikomanagements mit dem Schutz sensibler Daten.

Die Fragen, die ich mir als Chief Information Security Officer täglich stelle, sind: Welche unserer Daten sind für Hacker interessant? Und was wird ein potentieller Angreifer tun, um an diese Informationen heranzukommen? Für eine moderne Informationssicherheit besteht die Herausforderung darin, Angriffe frühzeitig vorherzusagen. Wir müssen uns in die Angreifer hineinendenken. So können wir Sensoriken entwickeln, um Bedrohungen frühzeitig zu erkennen und um in der Lage zu sein, darauf zu reagieren.

» Kann man sich auf einen Krisenfall vorbereiten, und wenn ja, wie?

« Man sollte sich auf jeden Fall vorbereiten. Wir entwickeln Krisenmechanismen und spielen mit den Mitarbeitern in Krisenübungen verschiedene Bedrohungsszenarien durch. Die Kunst besteht darin, eine Balance herzustellen zwischen technischen Maßnahmen, einem funktionierenden Risikomanagement und dem nötigen Risikobewusstsein. Denn wenn es um Informationssicherheit geht, darf man keinesfalls den menschlichen Faktor unterschätzen.

» Welche Rolle spielt der Faktor Mensch bei der Informationssicherheit?

« Ganz gleich, wie sicher wir Systeme gestalten und uns gegen Angriffe von außen abschotten, den Faktor Mensch darf man nie unterschätzen. Ich bin in meiner Funktion als CISO viel unterwegs. Was ich dabei in den Flughäfen dieser Welt sehe, ist für mich immer wieder erschreckend: Laptops, die unbeaufsichtigt herumstehen. Eingeschaltet. Fluggäste, die aktienkursrelevante Informationen ihres Arbeitgebers auf dem Bildschirm checken,



Welche Daten sind für Hacker interessant?

während Mitreisende über die Schulter mitlesen können. Ein Hauptanliegen moderner Informationssicherheit muss es deshalb konsequenterweise sein, die Mitarbeiter für einen verantwortungsbewussten Umgang mit Daten zu sensibilisieren und sicheres Verhalten zu schulen. Und so, wie die Informationssicherheit sich in Hacker hineinendenken muss, muss sie auch überlegen, was der Mitarbeiter will und braucht.

» Was bedeutet das konkret?

« Das bedeutet konkret: Sie müssen Sicherheitsmechanismen entwickeln, die funktionieren, die einfach sind und die den Mitarbeiter in seinem Arbeitsalltag nicht behindern. Dafür müssen Sie die IT-Systeme und die Arbeitsabläufe in den Abteilungen genau kennen. Denn wenn die Anwender die Sicherheitsmechanismen nicht akzeptieren, kann es schnell passieren, dass sie „kreative Lösungen“ finden, um lästige und scheinbar unnötige Umwege abzukürzen, die die IT-Sicherheit vorschreibt. Dieses Verhalten ist nur allzu menschlich. Erfolgreich sein wird die Informationssicherheit jedoch immer nur, wenn sie den menschlichen Faktor mitberücksichtigt. Denn menschliche Sicherheitslücken kann ich mit keiner Software dieser Welt schließen.

Save the Date

Compliance Berater

Betriebs-Berater Compliance



Deutsche Compliance Konferenz

28.-29. April 2016 | Hotel Scandic, Berlin
mit Verleihung Deutscher Compliance Preis

Compliance der Zukunft

Die richtungsweisende Konferenz für alle Compliance Officer

- **Corporate Compliance**

Compliance-Management im Mittelstand – Herausforderungen und Chancen

- **Risikoanalyse für Exportweltmeister**

Exportkontrolle und Sanktionen in der Praxis / Compliance in China / Neuerungen durch die 4. EU-Geldwäsche-Richtlinie – Umsetzungsstrategien für betroffene Unternehmen

- **Compliance Management**

Risikomanagement nach ISO 19600 / Compliance im Mittelstand nach der Einführung von ISO 19600 – Erfahrungen und Perspektiven aus der Praxis

- **Haftung und Aufsicht**

Bekämpfung der Korruption – Auswirkungen und Lösungsansätze für KMU / Kartellrecht in großen und kleinen Unternehmen – aktuelle Entwicklungen aus Gesetzgebung und Rechtsprechung

- **Branchen-Fokus**

Abgasskandal in der Automobilbranche – Lessons learned / Compliance Management in der Lieferkette: Third-Party-Management und Compliance-Due-Diligence

- **Datenschutz und IT-Compliance**

Neuerungen durch die EU-DS-GVO/ Neuerungen durch das IT-Sicherheitsgesetz für KMU und Erkennung und Vermeidung von Cybercrime

Melden Sie sich heute schon zur Deutschen Compliance Konferenz an und nutzen Sie den Early Bird € 699,- bis 31.12.2015!

Anmeldung unter:
www.deutsche-compliance-konferenz.de
Torsten Merk | Tel.: 069 7595-2783

Sie haben den CB – Compliance-Berater noch nicht im Abo?

Direkt hier bestellen und vergünstigt an der Deutschen Compliance Konferenz teilnehmen:
<http://www.ruw.de/abo/cb-printabo>

News

Studie belegt Chance zur Integritätskommunikation über die Marke

Die Studie „Kommunikationspotenziale in Compliance-Systemen deutscher Unternehmen“ des Konstanzer Instituts für Corporate Governance und der Münchner Agentur für Corporate Identity und Corporate Design zeigt, wie Fragen der Regelbefolgung auch für große Konzerne extern an Glaubwürdigkeit und intern an Überzeugungskraft gewinnen können. In der Studie haben Compliance-Verantwortliche von 64 Unternehmen zu den Erfolgsfaktoren im Integritätsmanagement Stellung bezogen.

Drei wesentliche Schlüsselfaktoren für funktionierende Compliance weist das Ergebnis der Studie aus: qualitativ hochwertige Schulungsprogramme; die Zurechnung von Compliance in die Linienverantwortung der Führungskräfte („Tone from the top“) und die Kommunikation. Hierbei kommt dem Zusammenspiel von unterschiedlichen Kommunikationsinstrumenten und -kanälen besondere Bedeutung zu. Die Studie zeigt, dass Compliance, die über die Marke kommuniziert wird, Chancen zur Förderung der Identifikation von Mitarbeitern in Unternehmen bietet.

www.htwg-konstanz.de

„Alles muss ans Licht“

Der italienische Investigativ-Journalist Gianluigi Nuzzi veröffentlicht ein neues Buch über das korrupte Finanzsystem des Vatikans. Laut eigenen Angaben hatte Nuzzi Zugang zu geheimen Dokumenten, die eine unglaubliche Misswirtschaft und Geldverschwendung durch die Kirchenführung belegen. Die vatikanische Finanzaufsicht arbeitet nun eng mit der italienischen Justiz zusammen.

<http://www.katholisch.de>

Weihnachten und der Umgang mit Benefits

Weihnachten steht vor der Tür, und es ist selbstverständlich, dass die Beschäftigten des Unternehmens mit Geschenken bedacht werden. Gutgemeinte Präsente können aber den betreffenden Mitarbeiter und das Unternehmen selbst in Schwierigkeiten bringen. Mit klaren Regeln zum Thema „Compliance“ lässt sich dies vermeiden.

Wer als Angestellter oder Beauftragter eines Unternehmens im geschäftlichen Verkehr einen Vorteil dafür fordert, sich versprechen lässt oder annimmt, dass er einen anderen beim Bezug von Waren oder gewerblichen Leistungen im Wettbewerb in unlauterer Weise bevorzugt, macht sich gemäß § 299 Strafgesetzbuch (StGB, Bestechlichkeit und Bestechung im geschäftlichen Verkehr) strafbar. Die Strafbarkeit besteht auch für Handlungen im ausländischen Wettbewerb.

Vorsicht, Falle

Trotz dieser Regelungen möchte kein Unternehmen unhöflich sein oder als übertrieben korrekt erscheinen. Deshalb wird den Beschäftigten die Annahme von Geschenken bzw. Einladungen erlaubt, sofern der Wert einen bestimmten Betrag nicht übersteigt. Nicht selten wird hier eine Wertgrenze von 30 bis 50 Euro für Geschenke und



Korrektur Umgang mit Geschenken ist unerlässlich.

bis zu 100 Euro für Essenseinladungen bzw. Einladungen zu Veranstaltungen empfohlen.

Aber Vorsicht! Ausschlaggebender Grund für die Strafbarkeit ist nicht die Zuwendung an sich bzw. deren Wert, sondern das Vorliegen einer Unrechtsvereinbarung. Der Mitarbeiter muss den Zuwendenden „in unlauterer Weise“ bevorzugen wollen – der Wert der Zuwendung spielt dabei eine zweitrangige Rolle.

Im Fall eines Strafverfahrens untersuchen die Gerichte zwar auch den konkreten Wert der Zuwendung, feste betragsmäßige Bagatellgrenzen gibt es aber nicht. Entscheidend ist immer die Absicht, die hinter dem Handeln steckt. Hier sind der Anlass des Geschenks, die Position und der Status des Empfängers sowie der Zusammenhang zur beruflichen Tätigkeit entscheidend. Auch die Transparenz und die Branchenüblichkeit spielen eine bedeutende Rolle.

Der Arbeitgeber darf kündigen

Hat sich ein Mitarbeiter wegen Korruption strafbar gemacht, so hat der Arbeitgeber das Recht, das Beschäftigungsverhältnis – ggf. auch außerordentlich – zu kündigen. Der Inhaber eines Betriebes begeht ggf. nach § 130 Ordnungswidrigkeitengesetz (OWiG) eine Ordnungswidrigkeit, wenn er vorsätzlich oder fahrlässig die notwendigen Aufsichtsmaßnahmen unterläßt. Die Bußgelder können bis zu 10 Millionen Euro erreichen.

Klare Regeln

In der Praxis empfiehlt es sich deshalb eine klare Wertgrenze festzusetzen (für Geschenke etwa 35 Euro). Es ist ratsam, eindeutig klarzustellen, dass Zuwendungen unterhalb dieser Grenze nur dann unbedenklich sind,

wenn keine besonderen Umstände hinzukommen (Beispiel: der Mitarbeiter fühlt sich „bestochen“). Hat ein Mitarbeiter Bedenken, sollte er sich sofort an den Vorgesetzten wenden. Erhält ein Mitarbeiter ein Geschenk in einem deutlichen höheren Wert, sollte dieses der Compliance-Abteilung gemeldet und dort abgegeben werden. Von dort aus kann dann eine Spende veranlasst werden. Auch kann ein Unternehmen Kunden und Geschäftspartner darüber informieren, dass statt Geschenken um eine wohltätige Spende gebeten wird.

Die Kontrolle dieser Regeln sollte jedes Unternehmen gewährleisten, und zwar durch Auswahl und Überwachung des zuständigen Personals und Schulung aller Mitarbeiter. Ist es zu einem Verstoß gekommen, sollte kein Arbeitgeber ein Auge zudrücken, sondern das Fehlverhalten sofort rigoros (beispielsweise mit einer Abmahnung) sanktionieren.

CSZ

Veranstaltungen

30.11.2015, München

- **Seminar zu Mittelstandsspezifischen Compliance-Risiken und dem Umgang mit Compliance-Klauseln:** Compliance Academy GmbH

07.12.2015, Köln

- **Aufbau einer Compliance-Organisation (Seminar):** Management Circle AG

09.12.2015, Köln

- **Campus Day zum Thema Compliance-Haftung und Berichtswege bei Einbindung des Aufsichtsrats:** Rheinische Fachhochschule Köln

19.01.2016, Hamburg

- **Neue Entwicklungen im chinesischen Steuer- und Wirtschaftsrecht:** Chinacademy

28.01.2015, Frankfurt am Main

- **Erfolgskontrolle der Compliance Kommunikation:** Fraport AG, Frankfurt Airport

02.02.2015, Hamburg

- **Auswirkungen der EU-Datenschutzgrund-VO auf den Datenschutz, auch im Gesundheitsbereich:** Hochschule Fresenius

IMPRESSUM

Verlag: FRANKFURT BUSINESS MEDIA GmbH
Der F.A.Z.-Fachverlag
Frankenallee 68–72, 60327 Frankfurt am Main
E-Mail: verlag@frankfurt-bm.com
HRB Nr. 53454, Amtsgericht Frankfurt am Main
Geschäftsführer: Torsten Bardohn, Dr. André Hülsbömer
Vorsitzender der Geschäftsleitung: Bastian Frieß
Redaktion
Gunther Schilling (Verantwortlich)
Telefon: (069) 75 91-21 96, Telefax: (069) 75 91-32 24
E-Mail: gunther.schilling@frankfurt-bm.com
Verantwortlich für Anzeigen
Dorothee Groove, Objektleitung Compliance
Telefon: (069) 75 91-32 17, Telefax: (069) 75 91-24 95
E-Mail: dorothee.groove@frankfurt-bm.com

Herausgeber: Boris Karkowski

Mitherausgeber
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH,
KPMG AG, SAI Global

Fachbeirat der Online Zeitschrift Compliance
Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Paul Hartmann AG; Ralf Brandt, LTS Lohmann Therapie-Systeme AG; Otto Geiß, Fraport AG; Mirko Haase, Adam Opel AG; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Olaf Kirchhoff, Mitutoyo Europe GmbH; Torsten Krumbach, Sky AG; Dr. Karsten Leffrang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Corpus Sireo Holding; Dr. Dietmar Prechtel, Osram GmbH; Alexander von Reden, Bosch-Siemens Hausgeräte GmbH; Jörg Siegmund, TSG Technologie Services GmbH; Elena Späth, Klöckner & Co SE; Dr. Martin Walter, Telekom Austria Group; Heiko Wendel, Rolls-Royce Power Systems AG; Dietmar Will, Audi AG.

Jahresabonnement: kostenlos

Erscheinungsweise: monatlich (10 Ausgaben im Jahr)

Layout
Daniela Seidel, FRANKFURT BUSINESS MEDIA GmbH

© Alle Rechte vorbehalten.

FRANKFURT BUSINESS MEDIA GmbH, 2015.

Die Inhalte dieser Zeitschrift werden in gedruckter und digitaler Form vertrieben und sind aus Datenbanken abrufbar. Eine Verwertung der urheberrechtlich geschützten Inhalte ist ohne vorherige schriftliche Zustimmung des Verlages unzulässig und strafbar, sofern sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Es ist nicht gestattet, die Inhalte zu vervielfältigen, zu ändern, zu verbreiten, dauerhaft zu speichern oder nachzudrucken. Insbesondere dürfen die Inhalte nicht zum Aufbau einer Datenbank verwendet oder an Dritte weitergegeben werden.

Haftungsausschluss: Alle Angaben wurden sorgfältig recherchiert und zusammengestellt. Für die Richtigkeit und Vollständigkeit des Inhalts von „Compliance“ übernehmen Verlag und Redaktion keine Gewähr. Für unverlangt eingesandte Manuskripte und unverlangt zugestellte Fotografien oder Grafiken wird keine Haftung übernommen.

Personalwechsel



Credit Suisse

Credit Suisse: Lara Warner ist Chief Compliance and Regulatory Affairs Officer

Lara Warner ist seit dem 22. Oktober Chief Compliance and Regulatory Affairs Officer der Credit Suisse. Sie ist neues Mitglied der Geschäftsleitung und künftig konzernweit für alle Compliance-Themen verantwortlich. Dabei handelt es sich um ein Ressort und eine Position, die der Konzern neu geschaffen hat. Dieser Schritt ist

Bestandteil einer umfassenden Neuordnung der Konzernleitung, die in diesem Rahmen von zehn auf zwölf Personen erweitert wird. Lara Warner ist US-Staatsbürgerin, wird aber ihre Aufgaben von Zürich aus erledigen. Sie kam 2002 zu Credit Suisse, zuvor war sie bei Lehman Brothers und AT&T beschäftigt.

Torsten Krumbach verlässt Sky und wechselt als Compliance Officer zu Bosch Sicherheitssysteme GmbH



private

Torsten Krumbach wird Ende 2015 Sky verlassen. Er wechselt zum 1. Januar 2016 als Compliance Officer zur Bosch Sicherheitssysteme GmbH. Krumbach ist Rechtsanwalt und wurde 2011 auf die Position des Group Compliance Officers bei der zwischenzeitlich zur Sky Deutschland AG umfirmierten Premiere AG berufen. Dort war er zuletzt Leiter der Internen Revision und zuvor sieben Jahre bei der Bayerischen Landesbank in den Bereichen Risikomanagement, Compliance, Geldwäscheprävention und Internen Revision tätig. Torsten Krumbach ist Dozent an der Frankfurt School of Finance & Management im Rahmen des Zertifikatsstudiengangs zum Certified Compliance Professional (CCP) sowie Referent bei anderen Compliance-Veranstaltungen und hat diverse Fachbeiträge zum Thema Compliance veröffentlicht. Krumbach ist Mitglied des Präsidiums des Berufsverbands der Compliance Manager (BCM) sowie Mitglied des Fachbeirats von Compliance.

Agricultural Bank of China: Rieth übernimmt Abteilungen Compliance und Antigeldwäsche



Agricultural Bank of China

Andreas Rieth (41) ist seit dem 1. Oktober Head of Legal & Compliance AML bei der Agricultural Bank of China, Frankfurt Branch. Er übernimmt die Leitung der Rechtsabteilung und ist zugleich Compliance- und Geldwäschebeauftragter. Vor seinem Wechsel war Andreas Rieth bei der ING Diba Syndikus in der Abteilung Vorstandsekretariat/Recht, Ressort „B2B / Vertragswesen“.

Boehringer: Dr. Martin Schwarz ist künftig für Compliance verantwortlich



Boehringer

Seit Oktober dieses Jahres leitet Dr. Martin Schwarz (39) die Bereiche Recht und Compliance beim Pharmakonzern Boehringer Ingelheim. Als General Counsel ist er Nachfolger von Dr. Andreas Neumann; dieser hatte die Funktion seit 2011 inne und wechselt zum 1. Oktober in die Unternehmensleitung. Schwarz ist künftig für 250 Juristen weltweit zuständig, die die Bereiche Recht und Compliance verantworten.

Stephanus-Stiftung hat einen neuen Compliance-Verantwortlichen



private, Foto: Anna Sauniger

Roland Heller (45) ist seit dem 1. September Leiter Recht & Compliance bei der Stephanus-Stiftung in Berlin. Er berichtet an den Vorstandsvorsitzenden des gemeinnützigen Dienstleistungsunternehmens, Pastor Torsten Silberbach. Heller war zuvor seit 2002 in verschiedenen Positionen für KPMG tätig, zuletzt als Director Risk Management/Rechtsabteilung.

SOS-Kinderdörfer weltweit ordnen Vorstand neu

Nach einer Amtszeit von 29 Jahren hat Helmut Kutin (74) den Vorstandsvorsitz der SOS-Kinderdörfer weltweit abgegeben. Als seinen Nachfolger wählte die Mitgliederversammlung Dr. Wilfried Vyslozil (57), der schon seit 2010 stellvertretender Vorsitzender des Vereins mit Sitz in München ist. Neu im Vorstand der SOS-Kinderdörfer weltweit ist Petra Horn (53), die von Düsseldorf aus Partnerschaften mit Stiftungen,

Family Offices und Unternehmen koordiniert. Weiterhin ist Ulla Sensburg (48) im Vorstand zuständig für Finanzen, Transparenz und Compliance. Zum Vorsitzenden des Aufsichtsrats wurde Dr. Christoph Marc Pressler (57), Rechtsanwalt in München, gewählt.

Deutsche Bank beschließt personelle Neuordnung

Die Deutsche Bank verändert ihren Konzernaufbau und ihre Führungsstruktur grundlegend. Dabei werden die Konzernsparten neu zugeschnitten. In diesem Zusammenhang wird Stephan Leithner auf eigenen Wunsch mit Wirkung zum 31. Oktober 2015 den Vorstand verlassen.



Deutsche Bank

Sylvie Matherat (derzeit Leiterin Government & Regulatory Affairs bei der Deutschen Bank und ehemaliges Mitglied des Direktoriums der Banque de France) übernimmt als Chief Regulatory Officer die neue Vorstandsverantwortung für die Bereiche Regulierung, Compliance und den Kampf gegen die Finanzkriminalität. Die Generalbevollmächtigte Nadine Faruque, die global für Compliance verantwortlich ist, wird an Matherat berichten.



Deutsche Bank

Karl von Rohr, bisher Chief Operating Officer für das globale Management der Regionen, wird als Chief Administrative Officer die Vorstandsverantwortung für Corporate Governance und das Personalressort übernehmen. Er wird damit Arbeitsdirektor der Deutsche Bank AG. Außerdem verantwortet von Rohr künftig auch den Rechtsbereich, für den bislang der Ko-Vorstandsvorsitzende John Cryan verantwortlich zeichnete. John Cryan übernimmt die Vorstandsverantwortung für die Restrukturierungseinheit NCOU.