

Inhalt



Aufmacher

Roundtable Compliance bietet handfeste Praxistipps zum CEO-Fraud

Am 27. März fand der Roundtable Compliance erstmals unter Federführung der dfv Mediengruppe und in Zusammenarbeit mit Beiten Burkhardt statt.

Praxis



CEO-Fraud vermeiden – Awareness im Unternehmen schaffen

Das perfekte Zusammenspiel aus Social Engineering und Cyber Crime führt immer häufiger zu millionenschweren Betrugsfällen, erklärt Kriminalhauptkommissar Stefan Becker.

5 Zwei Jahre ISO 19600 – Eine Bestandsaufnahme

Recht



Unternehmen müssen sich auf die Datenschutzgrundverordnung vorbereiten

Noch gut ein Jahr, spätestens dann müssen alle Unternehmen in Europa auf die Datenschutzgrundverordnung (DSGVO) vorbereitet sein.

10 Compliance-Management als Aufgabe der Personalabteilung

International



Compliance-Herausforderungen und Lösungsansätze in der Schweiz, Deutschland und Österreich

Rechtliche Risiken gehören heute zu den größten Risiken für Compliance-Praktiker, wie Dr. Helke Drenckhan in unserer Beitrags-Reihe zu übergreifenden Themen in der DACH-Region beschreibt.

Karriere

6 Personalwechsel

6 Hochrangige EU-Politiker wechseln häufig ins Lobbying

Hochaktuell!

Kapitalanlage-recht



KAGB – Kapitalanlagegesetzbuch
Juni 2016, Frankfurter Kommentar,
5.059 S. in 2 Halbbänden, Geb.
ISBN: 978-3-8005-1570-7
€ 529,-

R&W
Fachmedien Recht und Wirtschaft

dfv Mediengruppe 069/7595-2722 | buchverlag@ruw.de | www.shop.ruw.de

Roundtable Compliance bietet handfeste Praxistipps zum CEO-Fraud

Am 27. März fand der Roundtable Compliance erstmals unter Federführung der dfv Mediengruppe und in Zusammenarbeit mit Beiten Burkhardt statt. Zum Thema „CEO-Fraud“ hatte Jörg Bielefeld, Partner bei Beiten Burkhardt, interessante Referenten in die Räumlichkeiten der Kanzlei eingeladen.

Wie schütze ich mein Unternehmen vor dem sogenannten „CEO-Fraud“? Wie kann meine Hausbank helfen, wenn eine Zahlung durch einen Betrug veranlasst wurde, und welche Rolle spielt der Faktor Mensch im eigenen Unternehmen bei solchen Betrugsfällen?

Diese und weitere spannende Fragen rund um den Chef-Betrug diskutierten anlässlich des Roundtables Compliance unter der Moderation von Jörg Bielefeld die Referenten Stefan Be-

cker, Kompetenzzentrum Cybercrime, LKA Nordrhein-Westfalen, Ramon Schürer, Deutsche Bank AG, und Peter Zawilla, Geschäftsführer FMS Fraud & Compliance Management Services GmbH, mit gut 70 Gästen aus Unternehmen, Banken und Versicherungen. Denkanstöße zur Bewertung der eigenen Unternehmenskultur und anschauliche Praxistipps dominierten die Vorträge der drei Referenten. Die Resonanz des Auditoriums war aufgrund der häufig schnellen und einfachen Um-

setzbarkeit der Vorschläge durchweg positiv. Beim anschließenden Get-Together nutzten nahezu alle Teilnehmer noch die Gelegenheit zum intensiven persönlichen Austausch.

Lesen Sie in dieser und den kommenden Ausgaben ausführliche Berichte zu den jeweiligen Themenschwerpunkten der Veranstaltung. Den Auftakt macht in dieser Ausgabe ein Bericht zum Vortrag von Kriminalhauptkommissar Stefan Becker auf [Seite 4](#). *chk*



Kriminalhauptkommissar Stefan Becker zeigte die Dimensionen der Betrugs-Masche auf.



Teilnehmer aus Unternehmen, Banken und Versicherungen zeigten besonderes Interesse an den praktischen Konsequenzen des CEO-Fraud.



Die Referenten führten angeregte Diskussionen mit den Teilnehmern.





2. Compliance Solutions Conference

31. Mai 2017 in Köln

 Das Compliance-Event → Kostenfrei anmelden

- + Antworten auf Ihre aktuellen Compliance-Herausforderungen
- + Persönlicher Austausch unter Compliance-Experten
- + Von Trends und Best Practices führender Anbieter lernen
- + Lösungsanbieter für den gesamten Compliance-Prozess



Kostenfrei anmelden

lexisnexis.de/compliance-event



CEO-Fraud vermeiden – Awareness im Unternehmen schaffen

Das perfekte Zusammenspiel aus Social Engineering und Cyber Crime führt immer häufiger zu millionenschweren Betrugsfällen in deutschen Unternehmen. In seinem Auftaktvortrag zum Roundtable Compliance beschrieb Kriminalhauptkommissar Stefan Becker die Ergebnisse aus seinen zahlreichen Fällen im Bereich CEO-Fraud und gab handfeste Tipps für eine wirksame Prävention in den Unternehmen.

Gleich zu Beginn seines Vortrags stellte Stefan Becker klar: „Es ist kein einziger Fall bekannt, in dem jemand aus der Buchhaltung mit den Tätern kooperiert hätte.“ Im Gegenteil: „Die betreffenden Personen, die im Unternehmen gehandelt haben, sind suizidgefährdet.“ Damit wird schnell deutlich, dass nicht nur das Unternehmen durch den finanziellen Schaden zum Opfer geworden ist. Auch die Mitarbeiter, die eine schadensursächliche Zahlung vornehmen, sind trotz oder gerade wegen ihrer gewissenhaften Arbeitsauffassung zum Opfer geworden.

Doch, wie schaffen es die Täter, so geschickt zu täuschen? Aus Beckers Sicht sind die Vorbereitungshandlungen der Täter – das Ausspähen der Firmeninterna – dabei mindestens genau so entscheidend, wie die Durchführung der eigentlichen Tat. Oft geben bereits öffentlich einsehbare Informationen über die Unternehmen den Tätern wertvolle Hinweise zur Tatvorbereitung und -durchführung. Dazu gehören Informationen darüber, wann der CEO verreist ist, wer Überweisungen veranlassen darf, welche Projekte das Unternehmen aktuell plant, welche Sicherheitsmechanismen im Unternehmen bestehen und wie das Wording im Unternehmen ist. „Manches davon finden die Täter durch harmlos wirkende Anrufe im Unternehmen Wochen vor der Tat heraus“, so Becker.

„Im nächsten Schritt bauen die Täter potemkinsche Dörfer“, erklärt er. Sie schaffen also eine täuschend echte Kulisse für ihre Tat. Hierzu werden zum Beispiel gefälschte Webpräsenzen von Anwaltskanzleien angelegt. „Echte Webpräsenzen werden einfach kopiert und unter einer leicht geänderten Webadresse verwendet“, beschreibt Becker diesen Vorgang. Zentraler Bestandteil der Vorbereitungen sind gefälschte E-Mail-Accounts, erläutert der Kriminalhauptkommissar und zeigt eindrucksvoll, wie einfach es ist, E-Mails unter dem Namen „Angela Merkel“ zu versenden. Denn der Name, der als Absender im Namensfeld der E-Mail erscheint, muss längst nichts zu tun haben mit der echten Absenderadresse, die verwendet wird.

So knüpfen die Täter in den meisten Fällen den Kontakt über eine solche gefälschte E-Mail, die im Absender den Namen des CEO trägt. Kurz und knapp wird dann in diesen E-Mails behauptet, dass eine absolut vertrauliche Transaktion bevorstehe. Die Kommunikation dürfe ausschließlich per Mail erfolgen und der angesprochene Mitarbeiter sei die einzig involvierte Person in dieser Sache.



Stefan Becker ist als Kriminalhauptkommissar im Kompetenzzentrum Cybercrime im Landeskriminalamt NRW tätig. Mit der Bekämpfung von Computerkriminalität befasst er sich seit 1999.

Nicht selten werden Sanktionen oder Vertragsstrafen in Aussicht gestellt, falls der Mitarbeiter die Überweisung nicht mit der geforderten Vertraulichkeit vornimmt.

Gerade in Unternehmen, die hierarchisch strukturiert sind und in denen die Mitarbeiter sich, aus Furcht anzuecken, nicht gerne im CEO-Büro rückversichern, führe diese Masche zum Erfolg. „Solvente Mittelständler sind daher besonders im Fokus“, berichtet Becker. Die Anfälligkeit für den CEO-Fraud ist also ganz klar auch eine Frage der Unternehmenskultur, stellt Becker fest und verweist auf seinen Co-Referenten Peter Zawilla, Geschäftsführer der FMS Fraud & Compliance Management Services GmbH, der den „Faktor Mensch“ im Zusammenhang mit Betrugsmaschen beleuchtet (lesen Sie hierzu unseren Bericht in der kommenden Juni-Ausgabe von Compliance).

Auch wenn in manchen Fällen die Zahlung mit Hilfe der Hausbank angehalten (lesen Sie hierzu den Bericht zum Vortrag von Ramon Schürer, Deutsche Bank, in der kommenden Mai-Ausgabe von Compliance) oder mit Hilfe der Polizei zurückgeholt werden kann, steht für Kriminalhauptkommissar Becker natürlich im Vordergrund: „Schaffen Sie Awareness im Unternehmen. Informieren Sie Ihre Mitarbeiter.“ Aber auch einfache technische Lösungen können helfen: „E-Mails, die von außen kommen, können über die Server-Konfiguration als extern gekennzeichnet werden“, erklärt Becker.

Außerdem sollte kontrolliert werden, welche Informationen über das eigene Unternehmen öffentlich zugänglich sind. Wichtig auch: Was ist im Handelsregister zum Beispiel bezüglich Unterschriften veröffentlicht und was wird über den Aufenthalt der Firmenleitung und die Solvenz des Unternehmens bekannt gegeben?

Kommt es trotz aller Vorbereitung zum Betrug, läuft die Zeit: „Sobald Sie den Vorfall bemerken, informieren Sie als allererstes Ihre Hausbank, um die Zahlung anzuhalten“, appelliert Becker an die Teilnehmer des Roundtables Compliance. *chk*

Chef-Betrugsmasche CEO-Fraud

Beim sogenannten CEO-Fraud geben sich gut organisierte und vorbereitete Täter überzeugend als Geschäftsführer oder weisungsbefugte Entscheidungsträger eines Unternehmens aus. Dem Buchhalter eines Unternehmens wird durch mehrfache E-Mails und Anrufe vorgespielt, eine dringende und geheime Geldüberweisung müsse schnell und unauffällig durchgeführt werden. Die Täter bauen dabei großen Druck auf. Selbst erfahrene Buchhalter werden so zur Überweisung von Millionenbeträgen gedrängt – auch weil die Täter ihre Vorgehensweise stets individuell auf die Zielperson und deren Persönlichkeit abstimmen.

Mehr dazu lesen Sie auf den Internetseiten des [LKA NRW](#).

Zwei Jahre ISO 19600 – Eine Bestandsaufnahme

Die ISO 19600 – Ende 2014 als Standard für Compliance-Management-Systeme (CMS) veröffentlicht – ist inzwischen von Experten rezipiert und von Compliance-Verantwortlichen in Unternehmen umgesetzt worden. Dr. Jörg Viebranz zeigt auf, wie sich der Standard verbreitet hat und welche Schlüsse sich daraus für die weitere Entwicklung und Durchdringung der Compliance-Praxis ziehen lassen.

COMPLIANCE

Im Rahmen einer Befragung zu einer **Studie zu Compliance im Mittelstand** von Kerkhoff Risk & Compliance gaben 20 Prozent der mittelständischen Unternehmen an, ihr CMS nach ISO 19600 ausgerichtet zu haben. 17,1 Prozent orientierten sich an PS 980. Dies ist aufgrund der relativ kurzen Zeitspanne, die ISO überhaupt existiert, durchaus bemerkenswert. Noch deutlicher fällt die Antwort aus, wenn Unternehmen ohne CMS befragt werden, an welchem Standard sie ein CMS ausrichten würden. 38,9 Prozent sagen, dass sie sich an ISO orientieren würden. Nur 16,7 Prozent würden PS 980 als Grundlage wählen. Bei der Ausrichtung und als Orientierungshilfe scheint sich ISO 19600 also in der Praxis durchzusetzen. Laut einer Umfrage zur **EY-Studie „Existing Practice in Compliance 2016“** haben sich 10 Prozent der befragten Unternehmen nach einem Standard zertifizieren lassen, der nicht PS 980 ist. Den größten Anteil daran hat ISO. Einer ähnlichen Umfrage im Rahmen einer **PWC-Studie zur Wirtschaftskriminalität** zufolge, haben sich im Jahr 2015 bereits 9,2 Prozent (eigene Berechnungen basierend auf Daten der PWC-Studie, S. 80) der befragten Unternehmen nach ISO 19600 zertifizieren lassen. Es zeigt sich, dass es bei der Zertifizierung ebenfalls einen signifikanten Unterschied zwischen kleineren und größeren Unternehmen gibt. Unternehmen mit weniger als 5.000 Mitarbeitern haben gerade einmal zu 5,82 Prozent ihr CMS nach ISO auditieren lassen. Bei den Unternehmen mit mehr als 5.000 Mitarbeitern sind es 16,38 Prozent. Bei letzteren hat die ISO einen fast genauso hohen Anteil an Auditierungen wie PS 980. Die größten Unternehmen sind zu 17,53 Prozent nach PS 980 auditiert, die kleineren sogar zu 22,59 Prozent (eigene Berechnungen basierend auf Daten der PWC-Studie, S. 80). Bei großen Unternehmen scheinen beide Normen annähernd gleich beliebt zu sein.

Der große Unterschied ist besonders bei kleineren Unternehmen zu finden. Mehr als viermal so viele sind nach PS 980 zertifiziert als nach ISO

ISO 19600: Was hat der Compliance-Standard unterm Strich bisher gebracht?

19600. Möglicherweise wollen sie erst bei anderen Unternehmen beobachten, ob sich der Standard durchsetzt. Eine weitere Erklärung könnte sein, dass die Vertragskonditionen der kleineren Unternehmen mit ihren Kunden regelmäßig den Nachweis bestimmter Zertifizierungen des CMS verlangen. Sollten die Klauseln bestimmte Standards wie den PS 980 vorsehen, weil die Verträge älter sind und die ISO bei Vertragsschluss noch nicht veröffentlicht war, könnte dies den großen Unterschied bei der Zertifizierung von kleineren Unternehmen erklären. Wenn in Zukunft entsprechende Verträge die ISO einschließen, könnte diese Lücke geschlossen werden. Dies würde zu einer weiteren Verbreitung und Etablierung der ISO-Norm führen. Unterstützt



Dr. Jörg Viebranz war bis Ende 2016 Compliance Partner bei Idox Compliance in Berlin, wo er mittelgroße und größere Unternehmen bei der Einführung und der Optimierung von Compliance-Management-Systemen beriet. Inzwischen ist er Compliance Officer bei einem deutschen M-Dax Konzern.

wird dies durch die Tatsache, dass 15 Prozent der Unternehmen es für wahrscheinlich oder sehr wahrscheinlich halten, sich laut den Befragungen zur PWC-Studie in den kommenden zwei Jahren nach ISO 19600 zertifizieren lassen zu wollen. 29 Prozent sind noch unentschieden.

Auch wenn einzelne Gruppen durchaus Kritik anbringen, scheinen sich Experten und Praktiker darin einig zu sein, dass die ISO 19600 eine gute Orientierung für Unternehmen bietet, um ihr Compliance-Programm aufzubauen. Die Attraktivität dieser Norm lässt sich u. a. durch die Geschwindigkeit belegen, mit der ISO 19600 adaptiert wurde. Ungefähr die Hälfte aller Unternehmen hat sich inzwischen aktiv mit ihr auseinandergesetzt und ein bemerkenswerter Anteil von rund einem Zehntel hat sich bereits zertifizieren lassen. Auch für die nahe Zukunft wird dieser Trend sicherlich noch anhalten. Die ISO scheint vor diesem Hintergrund auf einem guten Weg zu sein, eine weithin akzeptierte Grundlage und Orientierungshilfe für die Einrichtung eines CMS bereitzustellen.

Dr. Jörg Viebranz

Mehr zum Thema lesen Sie im kostenlosen **E-Book** von Idox Compliance.

Personalwechsel

Kurt Michels neuer Group Chief Compliance Officer bei VW



Volkswagen AG

Dr. Kurt Michels (46) ist zum 1. April als Group Chief Compliance Officer (CEO) zum Volkswagen-Konzern gewechselt. Michels folgt Dr. Frank Fabian (50), der zum April zur Wolfsburg AG wechselte und dort Sprecher des Vorstands ist. Michels war zuvor bei der Daimler-Benz AG, wo er bereits 1998 als Syndikusanwalt einstieg. 2011 wurde er zum CEO für die Sparte Trucks und Vans bei Daimler berufen, 2013 auch für die Sparte Busse. In dieser Funktion war er für die Entwicklung und Implementierung eines Compliance-Programms zuständig. Michels ist nicht der erste Compliance-Experte, der von Daimler zu Volkswagen wechselt. Die ehemalige Richterin des Bundesverfassungsgerichts, Dr. Christine Hohmann-Dennhardt, die erst Anfang

2016 in den VW-Vorstand gewechselt und schon zum 31. Januar 2017 wegen „unterschiedlicher Auffassungen über Verantwortlichkeiten und die künftigen operativen Arbeitsstrukturen“ wieder ausgeschieden war, leitete bei Daimler seit Februar 2011 das Ressort Compliance.

Charlotte Hogg als Vize-Chefin der Bank of England zurückgetreten



Bank of England

Charlotte Hogg stolperte nach nur 14 Tagen im Amt über einen Interessenkonflikt und trat Mitte März als Vizechefin der Bank of England zurück. Hogg, die bereits seit 2013 für die Zentralbank tätig war, hatte nicht offengelegt, dass ihr Bruder in einer höheren Position bei der von der Notenbank beaufsichtigten Geschäftsbank Barclays arbeitet. Sie hatte damit offenbar den Verhaltenskodex der Bank verletzt, den sie selbst mit geschrieben hatte.

Hochrangige EU-Politiker wechseln häufig ins Lobbying

In einem Bericht über den Wechsel von ehemals hochrangigen EU-Vertretern in die Privatwirtschaft hat die Antikorruptionsorganisation Transparency International die Karrieren von 485 ehemaligen Mitgliedern des Europäischen Parlaments und 27 Vertretern, die aus der Kommission ausgeschieden sind, analysiert. Das Ergebnis: 30 Prozent aller Europaabgeordneten und sogar 50 Prozent der EU-Kommissare, die sich seit 2014 aus der Politik verabschiedet haben, arbeiten anschließend für Organisationen, die im EU-Lobbyregister geführt sind. Wer genau wo nach seiner Zeit auf dem Brüsseler Parkett angeheuert hat, zeigt im Detail die interaktive Datenbank EU Integrity Watch von Transparency International.



EU-Parlament in Straßburg

**HAUFE.
AKADEMIE**

Alles wird leicht.

Compliance-Risiken nachhaltig reduzieren mit den Seminaren der Haufe Akademie!

Compliance-Management I: Einführung eines Compliance-Management-systems (CMS)

Seminar, 2 Tage
06.-07.07.17 | Berlin
09.-10.10.17 | Frankfurt a. M.

Mehr Infos und Buchung unter www.haufe-akademie.de/35.60

Compliance-Management II: Umsetzung – Steuerung – Wirksamkeitskontrolle

Seminar, 2 Tage
02.-03.05.17 | Köln
08.-09.08.17 | Hamburg
18.-19.10.17 | München

Mehr Infos und Buchung unter www.haufe-akademie.de/35.67

www.haufe-akademie.de/compliance

In Kooperation mit dem Netzwerk Compliance e. V.

Unternehmen müssen sich auf die Datenschutzgrundverordnung vorbereiten

Noch gut ein Jahr, spätestens dann müssen alle Unternehmen in Europa auf die Datenschutzgrundverordnung (DSGVO) vorbereitet sein. Was das konkret bedeutet, erklärt Dr. Axel von Walter, Fachanwalt für IT-Recht und Fachanwalt für Urheber- und Medienrecht.

Wichtig sind besonders die umfassenden Dokumentationspflichten, die sich aus dem Grundsatz der Verantwortlichkeit („Accountability“) ergeben. Das Verantwortungsprinzip ist nicht nur eine Leerformel. Vielmehr räumt ihm die DSGVO durch damit verbundene Rechenschaftspflichten (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO) eine herausragende Stellung im neuen Regime der Datenschutzregelungen ein. Das Prinzip der „Accountability“ hat zur Folge, dass Unternehmen die Einhaltung der DSGVO dokumentieren und jederzeit nachweisen können müssen.

Es müssen „technische und organisatorische Maßnahmen“ (Art. 24 Abs. 1 DSGVO) getroffen werden, die die Einhaltung des Datenschutzes garantieren. Zudem müssen interne Prozesse überwacht und geprüft werden, um die ständige Einhaltung der Schutzstandards nachweisen zu können. Unternehmen können hier von Compliance lernen, um die neuen Pflichten mit bekannten Prozessen in Einklang zu bringen.

Das Wichtigste im Überblick

Die Datenschutzgrundverordnung (DSGVO) löst das bisherige Bundesdatenschutzgesetz (BDSG) ab und gilt als EU-weit verbindliche Regelung ab dem 25. Mai 2018. Die Verordnung regelt die Erhebung und Nutzung personenbezogener Daten. Sie gilt für alle Unternehmen, die in der EU ihren Sitz haben. Außerdem gilt die neue Regelung auch für Unternehmen, die in der EU am Markt tätig sind (Markortprinzip).

Neben bekannten Prinzipien wie Datensparsamkeit, Transparenz, Rechtmäßigkeit und Zweckbindung enthält die Verordnung auch neue Pflichten, etwa hinsichtlich Dokumentation und Betroffeneninformation, und gewährleistet deren Einhaltung durch die drastische Erhöhung des Strafrahmens.



Datenfluss: Unternehmen müssen sich schnellstmöglich an die DSGVO anpassen.

Die Verordnung benennt als konkrete Maßnahmen die datenschutzfreundliche Technik- und Verfahrensgestaltung („privacy by design“), sowie datenschutzfreundliche Voreinstellungen, die nur die Verarbeitung erforderlicher Daten gewährleisten („privacy by default“).

Das Prinzip der Verantwortlichkeit konkretisiert sich in dem nach Art. 30 DSGVO zu führenden Verarbeitungsverzeichnis. Dieses ähnelt dem Verarbeitungsverzeichnis, das Unternehmen schon heute nach §§ 4g Abs. 2, 4e BDSG führen.

In diesem Verzeichnis sind die Kategorien der verarbeiteten Daten, der Kreis der Betroffenen, der Verarbeitungszweck, die Datenempfänger, Übermittlungen in Drittländer sowie gegebenenfalls Löschfristen und die Beschreibung der Sicherungsmaßnahmen anzugeben. Neu ist, dass auch Auftragsdatenverarbeiter ein Verzeichnis zu führen haben (Art. 30 Abs. 2 DSGVO).

Im Unterschied zum Bundesdatenschutzgesetz (BDSG) entfällt das öffentliche Jedermann-Verzeichnis. Eine Pflicht zur Offenlegung der Verfahren besteht nun grundsätzlich nur noch gegenüber den Aufsichtsbehörden. Anders als bislang droht bei Fehlen des Verzeichnisses nun ein empfindliches Bußgeld.

Angesichts der Erhöhung des Bußgeldrahmens auf bis zu 4% des gesamten Jahresumsatzes (zumindest bei Verstößen gegen die Grundsätze der Verarbeitung oder die Betroffenenrechte, Art. 83 Abs. 5 DSGVO) und der Erweiterung bußgeldbewehrter Pflichten sollten Unternehmen der Accoun-

tability und den damit verbundenen Dokumentationspflichten eine erhöhte Priorität einräumen.

Die verpflichtende Folgenabschätzung nach Art. 35 DSGVO ist eine Risikoanalyse, die im Anwendungsbereich deutlich weiter reicht als die bisherige Vorabkontrolle nach § 4d Abs. 5 BDSG.

Die Folgenabschätzung ist erforderlich, wenn neue Technologien eingesetzt werden (Erwägungsgründe 89, 91), große Datenmengen (Erwägungsgrund 91) oder besonders sensible Daten (Art. 35 Abs. 3 lit. b DSGVO, Erwägungsgrund 91), wie etwa biometrische Daten, Gesundheitsdaten oder Daten über Straftaten, verarbeitet werden, bei Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c DSGVO, z.B. Videoüberwachung von Eingangsbereichen) oder wenn rechtsverbindliche Entscheidungen aufgrund von Personenbewertungen getroffen werden und diese Bewertungen auf automatisierter Datenverarbeitung basieren (Art. 35 Abs. 3 lit. a DSGVO, etwa Profilbildung).

Die Datenschutzbehörden müssen nach der DSGVO Positiv- und sollen Negativlisten für typische Fälle einer Datenschutz-Folgenabschätzung veröffentlichen (Art. 35 Abs. 4, 5 DSGVO). Diese Listen werden Regelbeispiele für die Erforderlichkeit (Positivliste) oder Entbehrlichkeit (Negativliste) einer Risikofolgenabschätzung geben.

Dr. Axel von Walter

Handlungsbedarf

Wichtig ist, dass Unternehmen schnell eine Bestandsaufnahme über alle Verarbeitungsprozesse machen und als Verarbeitungsverzeichnis dokumentieren. Aus dem Verarbeitungsverzeichnis lässt sich der weitere Handlungsbedarf, z. B. im Rahmen der Risikofolgenabschätzung ableiten.

Die Zeit drängt. Unternehmen sollten die Bestandsaufnahme bis Spätsommer 2017 abschließen, um über den Jahreswechsel den Anpassungsbedarf im Unternehmen, in Betriebsvereinbarungen, Verträgen und Policies zu ermitteln.



Dr. Axel von Walter ist Rechtsanwalt und Partner im Bereich IP/IT/TMT bei BEITEN BURKHARDT und Lehrbeauftragter an der Ludwig-Maximilians-Universität München für Medien- und Informationsrecht. Er berät Unternehmen u.a. umfassend im Bereich Datenschutz und Compliance und unterstützt aktuell zahlreiche Unternehmen bei der Implementierung der DSGVO.

mit Peter Schaar
und Dr. Carlo Piltz

Praxisseminar zum neuen Datenschutzrecht - ein Jahr bis zur DSGVO

Eine Veranstaltung der Zeitschrift **Kommunikation & Recht**, **Compliance Berater** und **reuschlaw** Legal Consultants

Frankfurt am Main, 16. Mai 2017

Montag, 15. Mai 2017

ab 18:30 Uhr **„Get-together“ der Konferenzteilnehmer**

Dienstag, 16. Mai 2017

09:30 – 09:55 **Registrierung**

09:55 – 10:00 **Begrüßung:**

Dr. Carlo Piltz und Torsten Kutschke

10:00 – 11:00 **Thematische Einführung:**

- Überblick zur DSGVO
- Einordnung in das bestehende gesetzliche Gefüge
- Wesentliche neue Regelungen
(Anwendungsbereich; Rechenschaftspflicht;
Auftragsverarbeitung; Betroffenenrechte;
Sanktionen)

Dr. Carlo Piltz

11:00 – 11:30 **Kaffeepause**

11:30 – 12:30 **(Neue) Pflichten des Verantwortlichen
und Auftragsverarbeiters:**

- Transparenz- und Informationspflichten
- Regelungen zur gemeinsamen Verantwortlichkeit
- Anforderungen an die Auftragsverarbeitung
- Datenschutz-Folgenabschätzung und vorherige
Konsultation

Dr. Carlo Piltz

12:30 – 13:30 **Gemeinsame Mittagspause**

13:30 – 15:00 **Internationale Datentransfers
unter der DSGVO**

- Probleme und Lösungsansätze, Peter Schaar

15:00 – 15:30 **Kaffeepause**

15:30 – 16:30 **Technischer und organisatorischer
Datenschutz:**

- Anforderungen an die Sicherheit der Verarbeitung
- Datenschutzpannen und Meldepflichten
- Verzeichnis von Verarbeitungstätigkeiten
- Privacy by Design und Privacy by Default

Dr. Carlo Piltz

16:30 – 17:00 **Gemeinsame Abschlussdiskussion**

zum BDSG-E und Ende des Seminars,
Dr. Carlo Piltz und Peter Schaar



Dr. Carlo Piltz

Rechtsanwalt bei Reusch Rechtsanwälte, Berlin; Zertifizierter Datenschutzbeauftragter (TÜV)



Peter Schaar

Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAI), Berlin; Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D. (2003-2013)



Torsten Kutschke

Chefredakteur Kommunikation & Recht, Gesamtverlagsleiter Fachmedien Recht & Wirtschaft, Deutscher Fachverlag GmbH

Empfohlener Teilnehmerkreis:

Unternehmensjuristen, Leiter und Mitarbeiter von Rechtsabteilungen, Rechtsanwälte, Datenschutzbeauftragte, Geschäftsführer, Leiter von IT-Abteilungen. Das Praxisseminar richtet sich an Teilnehmer, die in ihrer täglichen Arbeit mit dem Datenschutzrecht in Berührung kommen und mit der Umsetzung der Vorgaben der EU Datenschutz-Grundverordnung befasst sind.

Teilnahmebestätigung:

Sie erhalten eine Bestätigung über 5 Zeitstunden zum Nachweis Ihrer Fortbildung gemäß § 15 FAO.

Praxisseminar zum neuen Datenschutzrecht - ein Jahr bis zur DSGVO

Ab dem 25. Mai 2018 soll eine neue Ära des Datenschutzes in Europa anbrechen. Ab diesem Tag ist die EU Datenschutz-Grundverordnung (DSGVO) unmittelbar in allen Mitgliedstaaten anwendbar. Bisher geltendes nationales Datenschutzrecht spielt dann zum weit überwiegenden Teil keine Rolle mehr. Die DSGVO regelt den Umgang mit personenbezogenen Daten, sei es im B2C oder auch im B2B Bereich, erstmals durch ein einheitliches europäisches Gesetz. Die Zeit zur Umsetzung der DSGVO und Anpassung der eigenen Verarbeitungsprozesse in Unternehmen, Behörden, Vereinen und Verbänden läuft jetzt.

Dem europäischen Verordnungsgeber ist es ernst: die bei Datenschutzverstößen potentiell im Raum stehenden Bußgelder können bis zu 20 Mio. Euro oder gar 4 % des weltweiten Jahresumsatzes eines Unternehmens betragen. Betroffene Personen, deren Daten verarbeitet werden, erhalten zum Teil neue Rechte und datenverarbeitende Stellen sind u.a. dazu verpflichtet, Betroffene umfassender zu informieren die Einhaltung der Vorgaben der DSGVO nachzuweisen. Datenverarbeitende Stellen, mögen Sie eigenverantwortlich oder als Dienstleister agieren, werden in der DSGVO mannigfaltige, von der aktuellen Gesetzeslage teilweise abweichende, Verpflichtungen auferlegt.

In unserem Praxisseminar erhalten Sie eine Einführung in die DSGVO und einen schlaglichtartigen Blick auf wichtige Änderungen zum datenschutzrechtlichen status quo. Zudem werden wir mit Ihnen ausgewählte, spezielle Probleme bei der Anpassung des eigenen Datenschutz-Management-Systems und möglichen Strategien zur Umsetzung der Vorgaben der DSGVO behandeln.

Sie haben die K&R und den CB noch nicht im Abo?

Ja, ich möchte die „K&R - Kommunikation und Recht“ abonnieren.

Ja, ich möchte den „CB - Compliance Berater“ abonnieren.

Bitte liefern Sie ab sofort ab Heft _____

die K&R zum Jahresbezugspreis von 455,00 Euro, bzw. den CB zum Jahresbezugspreis von 464,00 Euro (Inland, inkl. Vertriebskosten und MwSt.).

Veranstaltungsort:

25 Hours Hotel by Levi's
Niddastr. 58
60329 Frankfurt am Main

Teilnahmegebühr:

449,00 Euro (zzgl. MwSt) Abonnenten der K&R und des CB
549,00 Euro (zzgl. MwSt) Normalpreis
Die Teilnahmegebühr bitten wir nach Erhalt der Rechnung zu überweisen.

Rabatte:

So sparen Sie intelligent:

Frühbucherrabatt

5 % bis Buchung zum 10. April 2017.

Mehrbucherrabatt

5 % bei Anmeldung von 3 oder mehr Teilnehmern einer Kanzlei/einer Institution/einer Behörde/einer Kammer ab dem 3. Teilnehmer (unabhängig vom Frühbucherrabatt).

Anmeldeschluss:

Eine frühzeitige Anmeldung wird empfohlen,
Anmeldeschluss ist der 10. Mai 2017.

Stornierung:

Die Anmeldung ist übertragbar. Bei Stornierung bis zum 02. Mai 2017 (Eingangsdatum) wird eine Bearbeitungsgebühr von 50,00 Euro zzgl. MwSt. erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

Hotelempfehlungen:

- 25 hours hotel by levi's
Niddastr. 58, 60329 Frankfurt am Main
Tel.: 069 25 66 77 266
- Clarion Collection Hotel
Taunusstr. 48-50, 60329 Frankfurt am Main
Tel.: 069 96 86 9890
- Leonardo Hotel Frankfurt City Center
Münchener Str. 59, 60329 Frankfurt am Main
Tel.: 069 24 23 30

Name/Vorname

Kanzlei/Firma

Straße

PLZ/Ort

Telefon

Datum/Unterschrift

zurück per Fax: 069 7595 1150

Ich nehme am Vorabendempfang teil

K&R/CB Kundennummer

E-Mail

Kontakt

Deutscher Fachverlag GmbH · Torsten Kutschke, Gesamtverlagsleiter Fachmedien Recht & Wirtschaft
Mainzer Landstraße 251 · 60326 Frankfurt · Tel: 069 7595 1151 · Fax: 069 7595 1150 · Torsten.Kutschke@dfv.de

Compliance-Management als Aufgabe der Personalabteilung

Um gute Compliance zu gewährleisten, sind alle Abteilungen eines Unternehmens gefragt, an dem internen Compliance-System mitzuwirken. Denn nur gelebte Compliance, ist auch richtige Compliance und kann wirksam Risiken im gesamten Unternehmen minimieren und so eine Haftung ausschließen.



Faktor Mensch: Auch der Personalbereich ist ein Rad im Getriebe der Konzern-Compliance.

Compliance kann je nach Auffassung und Perspektive sehr unterschiedlich definiert werden. Der risikobasierte Ansatz ist ganzheitlich und greift in punkto „Compliance als Verantwortung aller im Unternehmen“ eine sehr treffende Beschreibung auf: „Compliance is knowing what your risks are and ensuring your resources are appropriately allocated.“

Globale Personalsysteme und internationale Datentransfers, der Einsatz von Sozialen Medien, flexibler Personaleinsatz und nicht zuletzt die speziellen Anforderungen des deutschen Arbeitsrechts sind dabei eine tägliche Herausforderung der HR-Compliance. Um diese Anforderungen in den Griff zu bekommen, kann die Funktion der Personalabteilung (u. a. „Betreuung von Mitarbeitern“) genutzt werden, um Compliance voranzutreiben.

Eine zentrale Rolle spielt somit neben der Compliance-Abteilung vor allem die Personalabteilung. Hierbei ist insbesondere auch an die unterschiedlichen Berufsgruppen zu denken, wie bspw. dem HR-Relationship-Manager. Der Personalbereich ist

letztlich Schaltstelle für fast alle Unternehmensprozesse und ist vom „on-boarding“ des Mitarbeiters bis hin zum „off-boarding“ Sprachrohr auch in Sachen Leit- und Richtlinien des Unternehmens. Neben dem Management kommuniziert die Personalabteilung somit ganz unmittelbar, was die Corporate Identity des jeweiligen Unternehmens ausmacht. Im Idealfall bekommt der Mitarbeiter beim „on-boarding“ ein Handbuch mit den ihn betreffenden Regelungen für seine Arbeit ausgehändigt. Dies reicht von relevanten Betriebsvereinbarungen bis hin zum Code of Conduct. Nach dem „Einlass“ in die sog. Corporate World gibt es jedoch noch viele weitere Themen, welche die Personalabteilung in Sachen Compliance zu tun hat. Sie weist auch den Mitarbeiter auf regelmäßige Schulungen für den Fachbereich hin, wie bspw. zu internen Richtlinien. Auch dies stellt einen wesentlichen Teil des Compliance-Managements dar. So kann sichergestellt und gleichzeitig dokumentiert werden, dass Mitarbeiter die internen Anforderungen kennen und so Risikofelder eindämmen. Es wird damit eine erste Awareness geschaffen („know your risks“).

Zusätzlich existieren zahlreiche weitere Compliance-Themen für den Personalbereich, die es zu managen und zu kontrollieren gilt, wie u. a.: gesetzliche Anforderungen durch das AGG, BetrVG, TV; die korrekte Durchführung der Anwerbung von Mitarbeitern selbst, d. h. korrektes Verfahren und Ablauf, Dokumentationspflichten sowie Löschpflichten von Arbeitnehmerdaten; Arbeitszeit und Arbeitsschutz als auch der Einsatz von Selbstständigen oder die Handhabung der arbeitsrechtlichen Folgen bei Verstößen. Jüngstes Mitglied in der Familie der Compliance-Risiken ist die AÜG-Reform.

Hierzu kann es auch gehören bei internen Ermittlungen der Compliance-Abteilung zu unterstützen und als sog. Bindeglied die Kommunikation mit dem Betriebsrat in diesen Fällen aufzunehmen. All dies sind nicht nur Nebenprozesse, sondern elementare Bestandteile eines funktionierenden CMS. Gerade die Zusammenarbeit in Schnittstellenbereichen wird hierbei in der Praxis oftmals unterschätzt und führt zu unüberwindbaren Lücken im System. Der Personalbereich muss daher einen Beitrag zur „Konzern-Compliance“

liefern. Hierbei müssen insbesondere die Prozesse auf Grundlage gestiegener Anforderungen neu überdacht werden: HR-Compliance-Review.

Im Ergebnis sind daher Schnittstellen und Risikofelder des Personalbereichs zu prüfen. Anhand neu definierter Ziele und Vorgaben kann hierdurch ein nachhaltiges CMS entstehen und wirkliche Präventionsarbeit geleistet werden. In diesem Zusammenhang spielen nicht nur Gesetze und Richtlinien aus dem Bereich des Arbeitsrechts eine Rolle, sondern insbesondere auch der Bereich Datenschutz und die damit verbundenen Prozessstrukturen innerhalb der Fachabteilung (vgl. zu den neuen Compliance-Risiken im Beschäftigtendatenschutz den Aufsatz von Fladung im CB 2015, 364). Dies betrifft damit alle Management-, Kern- und Unterstützungsprozesse des HR-Bereichs, welche regelmäßig auch im Interesse der Abteilung durch ein Audit zu beleuchten sind.

Jasmin Fladung, LL.M., CAD-Institut

HR-Compliance

- Gute Personalarbeit ist ein wichtiger Faktor für den Erfolg von Compliance. Nur so können Prozesse gesteuert, überwacht und vor allem transparent bleiben.
- Ein CMS sollte keine bloße Beschränkung auf Compliance selbst sein, sondern eine gestaltende Unternehmensführung für alle Stakeholder. Damit wird eine Strategie für die Zusammenarbeit von Fachabteilungen umso bedeutender und unausweichlicher.
- Die Bereiche Personal, sowie Compliance, Datenschutz und auch der Betriebsrat sind in der Praxis gefordert gerade bei der Umsetzung von Richtlinien als auch bei Schulungen und der Kommunikation im Unternehmen auf ein einheitliches Vorgehen hinzuwirken. Dabei gilt es nicht nur Compliance zu managen und zu predigen, sondern ebenso als Führungskraft zu demonstrieren, wie Compliance gelebt wird. Dazu gehört es, nicht nur im Ernstfall eine Einladung auszuschlagen, sondern auch seine Tätigkeiten transparent zu gestalten; soweit dies sinnvoll und möglich ist.
- Eine absolute Perfektion und Überkontrolle ist nicht das erstrebenswerte Ziel. Die Risiken auf ein akzeptables Niveau zu reduzieren, ist die Kunst die Compliance ausmacht. Der Personalbereich als zentrale Mittlerstelle im Unternehmen kann beim Risikomanagement somit durchgängig unterstützen.

IMPRESSUM

Verlag

Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
UStIdNr. DE 114139662

Geschäftsführung: Angela Wisken (Sprecherin), Peter Esser, Markus Gotta, Peter Kley, Holger Knapp, Sönke Reimers

Aufsichtsrat: Klaus Kottmeier, Andreas Lorch, Catrin Lorch, Peter Ruß

Redaktion: Christina Kahlen-Pappas (verantwortlich),
Telefon: 069 7595-1153,
E-Mail: christina.kahlen-pappas@dfv.de

Unter Mitwirkung von CAD-Institut für Compliance, Arbeitsrecht und Datenschutz

Verlagsleitung: RA Torsten Kutschke,
Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de

Anzeigen: Iris Biesinger, Telefon: 069 7595-2713,
E-Mail: iris.biesinger@dfv.de

Mitherausgeber:

BEITEN BURKHARDT Rechtsanwaltskanzlei mbH,
KPMG AG, SAI Global

Fachbeirat der Online-Zeitschrift Compliance: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe 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, Bosch Sicherheitssysteme GmbH; Dr. Karsten Leffrang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Corpus Sireo Holding GmbH; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, BSH Hausgeräte GmbH; Jörg Siegmund, Ratiodata GmbH; 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: Grafisches Atelier, Deutscher Fachverlag GmbH

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.

Compliance
Berater



Deutsche Compliance Konferenz

28. Juni 2017

dfv Mediengruppe, Frankfurt am Main

Compliance der Zukunft

Die richtungsweisende Konferenz für alle Compliance Officer

CSR, Corporate Governance und Compliance • Auf dem Weg zur „CSR-Compliance“ – Neue Berichtspflichten und die Folgen • Compliance und M&A-Transaktionen • Compliance-Risikomanagement – Fokus Criminal Compliance • Cyber-Security, Datenschutz und IT-Compliance • „Damoklesschwert“ Tax Compliance • Kartellrechts-Compliance

Name: _____

Firma: _____

Position: _____

Abteilung: _____

Telefon: _____

E-Mail: _____

Ort: _____

Straße: _____

Fax: _____

Datum, verbindliche Unterschrift: _____

Ja, ich nehme an der Deutschen Compliance Konferenz 2017 teil.

- € 349,- als Abonnent des Compliance-Berater
- € 399,- als Behördenvertreter / Unternehmensjurist
- € 499,- regulärer Preis

5% Mehrbucherrabatt bei Anmeldung jedes weiteren Teilnehmers aus Ihrem Unternehmen.

- Ja, ich nehme an der Vorabendveranstaltung am 27. Juni 2017 teil.

Sie haben den CB noch nicht im Abo?

- Ja, ich möchte den CB – Compliance-Berater zum Jahresbezugspreis Inland € 464,- (inkl. Vertriebskosten und MwSt.) abonnieren. Bitte liefern Sie ab sofort.



- Ja, ich möchte den Titel „Compliance Management im Unternehmen“ für € 149,- bestellen. (2017, Handbuch, 930 Seiten, Geb., ISBN: 978-3-8005-1630-8)

Sonja Pörtner

dfv Mediengruppe | Compliance Berater
Tel.: 069 7595-2712 | Fax: 069 7595-1150
sonja.poertner@dfv.de

www.deutsche-compliance-konferenz.de

dfv Mediengruppe

Compliance-Herausforderungen und Lösungsansätze in der Schweiz, Deutschland und Österreich

Rechtliche Risiken – und da waren sich alle Wissenschaftler und Praktiker anlässlich einer Podiumsdiskussion im Rahmen der DACH-Compliance Tagung im Februar 2017 der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) in Winterthur (Schweiz) einig – gehören heute zu den größten Risiken. Dennoch werden sie oft unterschätzt und sind schwer zu beherrschen. In unserem zweiten Beitrag in der Reihe zu relevanten Themen für Compliance-Praktiker der DACH-Region, fasst Frau Dr. Helke Drenckhan zusammen, welche Compliance-Herausforderungen bleiben und welche hinzukommen werden.



Risiko: Compliance-Verantwortliche in der DACH-Region müssen manche rechtliche Klippe überwinden.

Compliance ist rechtliches Risikomanagement und diese Risiken zu minimieren, wird für die Unternehmen von heute immer wichtiger. Welche Risiken das in der Schweiz, Deutschland und Österreich sind, welche hinzu kommen werden und wie man diesen wirkungsvoll begegnen kann, diskutierten anlässlich der Dach-Compliance Tagung Arndt Harbecke, Chief Compliance Officer Landis+Gyr, Eric Soong, Group Head Compliance & Corporate Security, Schaeffler AG, Prof. Dr. Claudia Seitz, Professorin der Universität Basel und Rechtsanwältin, Dr. Katharina Hastenrath, Dozentin der ZHAW und Rechtsanwältin, Rudolf Schwab, Compliance Officer Telekom Austria und Thomas Pletscher, Geschäftsleitungsmitglied der *economiesuisse*.

Bei einem Blick auf die zu bewältigenden Compliance-Risiken sahen die Experten viele alte aber auch neue Bekannte. Einigkeit bestand, dass die Compliance-Klassiker Kartellrecht, Korruption und Wirtschaftskriminalität auch weiterhin im Spotlight bleiben. Die gesetzlichen und behördlichen Anforderungen steigen und die Bußen erreichen teilweise existentielle Ausmaße. Der Informations-

austausch der Behörden auf internationaler Ebene, insbesondere in Kartellverfahren, verschärft die Risiken für die Unternehmen zusätzlich.

Und auch die Gesetzgeber werden nicht müde, neue Regelungen zu erlassen und diese sogar mit extraterritorialer Wirkung auszustatten. Für die Zukunft zeichnen sich zudem neue Aufgaben, beispielsweise im Datenschutz ab. Mit der EU-Datenschutzgrundverordnung ergeben sich neue Herausforderungen. Diskutiert wurde, ob diese Themenfelder künftig in den Unternehmen separate Einheiten, beispielsweise ein Datenschutzbeauftragter, wahrnehmen werden. Die Experten wiesen außerdem auf das Thema Exportkontrolle hin, das

heute oft von den Mitarbeitern der Logistik oder in der Zollabteilung getragen und bearbeitet wird. Der Eindruck entstand, dass die Managementsysteme in der Exportkontrolle in den drei Ländern unterschiedlich in ihrem Reifegrad sind. Hier lässt sich eine Tendenz der Länder zu mehr staatlichen Kontrollen erkennen. Die Zukunft wird zeigen, ob die Unternehmen insofern doch stärker nachrücken müssen. Auch neue Risiken, wie der Modern Slavery Act aus Großbritannien, wird für Unruhe und zusätzliche Compliance-Maßnahmen sorgen. Teilweise entstand der Eindruck, dass staatliche Aufgaben auf die Unternehmen abgewälzt würden.

Auch bei der Frage, wie man diesen zunehmenden Risiken wirkungsvoll begegnen könne, waren Strömungen erkennbar. Betont wurde, dass es in der DACH-Region eine Tendenz zu einer verstärkten Integration der Compliance-Aufgaben in die Geschäftsprozesse gibt. Die „Dezentralisierung“ und Vernetzung des Compliance Managements soll bei den Mitarbeitern auch bewirken, dass Compliance als Hilfe zur Selbsthilfe und nicht als interne Polizei erfahren wird. Trotz aller Nähe zum Geschäft, bleibt der „tone from the top and the middle“ weiterhin richtungsweisend. Eine eindeutige Positionierung der Geschäftsleitung erleichtert allen Compliance Officern das Leben.

Lebhaft diskutiert wurde auch, ob es nicht schon organisatorisch falsch sei, wenn der Compliance Officer an den General Counsel berichten würde. Eine solche Organisation wäre einerseits nicht unabhängig und andererseits wären die Arbeitsweisen von Legal und Compliance sehr unterschiedlich. Wichtig sei zudem ein direkter Austausch mit dem Board. Ein klassisches Leiden benannten auch die Praktiker unter den Experten: Den Kampf um die notwendigen Ressourcen. Sparmaßnahmen verschonen regelmäßig auch die Compliance-Organisation nicht. Damit Compliance nicht nur ein Lippenbekenntnis bleibt, ist neben der finanziellen Ausstattung auch eine entsprechende Stellung in der Organisation erforderlich. Hier gibt es gerade in der DACH-Region an vielen Orten noch Nachholbedarf.

Hervorgehoben wurde auch, dass Compliance als rechtliches Risikomanagement Teil des unternehmensweiten Risikomanagementsystems sein sollte. Dies würde eine bessere und engere Zusammenarbeit auf der einen Seite und eine einheitliche Bewertung der Risiken auf der anderen Seite erfordern. Die verschiedenen Risikofunktionen, insbesondere Compliance, Legal, Risikomanagement, IKS, Qualität und die interne Revision müssten sich austauschen und die Verantwortlichkeiten bestimmen. Eine solche Zusammenarbeit würde zu mehr Transparenz und auch Effizienz führen.

Insgesamt bestätigte sich einmal mehr, dass der Compliance-Alltag auch in den kommenden Jahren herausfordernd und spannend bleibt.

Dr. Helke Drenckhan

Dr. Helke Drenckhan ist Dozentin für Compliance an der Zürcher Hochschule ZHAW (MAS Compliance, DAS Compliance im Personalwesen).



Die nächste **DACH-Compliance-Tagung** findet am 16. Februar 2018 in Winterthur statt.

Save the Date

**Betriebs
Berater**



2. Frankfurter Steuerkongress

28. September 2017 | 9.00 - 17.30 Uhr, Frankfurt am Main

Themen

- **Internationales Steuerrecht**
BEPS - Umsetzung in nationales Recht - Wo stehen wir?
- **Banken und Finanzindustrie**
Betriebsstättengewinnermittlung, Investmentsteuerreform
- **Unternehmenssteuerpolitik**
Globalisierung – Herausforderungen an die nationale und internationale Steuerpolitik in Zeiten zunehmenden Protektionismus und Steuerwettbewerbs
- **Verfahrensrecht, Steuerstreit und Compliance**
Tax Compliance Systeme: Erfahrungen aus der Praxis, Informationsaustausch
- **Konzern- und Unternehmenssteuerrecht**
Verlustverrechnung, Bilanzsteuerrecht, Umwandlungssteuerrecht und Organschaft

www.frankfurter-steuerkongress.de

Partner

**Baker
McKenzie.**

dfv Mediengruppe