Compliance

Die Zeitschrift für Compliance-Verantwortliche

September 2018

Inhalt

privat

Aufmacher

Die ideale Compliance-Welt
Die Moralisierung des Rechts ist im Aufwind, stellt Dr. Malte Passarge fest und sieht darin mit einer großen Portion Ironie die „ideale Compliance-Welt". Sehr ernst gemeint ist dagegen seine Beschreibung der – auch durch den technologischen Fortschritt getriebenen – Entwicklung hin zum Überwachungssystem für „unethisches Verhalten".

Praxis

BrianAJackson/iStock/Thinkstock

Cybercrime: Vom Opfer zum Täter – die Verantwortung des Managements
Chefbetrug bzw. CEO-Fraud ist inzwischen eine bekannte Masche. Trotzdem gelingt es den Betrügern weiterhin, vor allem mittelständische Unternehmen massiv zu schädigen. Für Unternehmen bedeutet diese Entwicklung vor allem eines: Ein Perspektivwechsel ist nötig!

Praxis

aurielaki/iStock/Thinkstock

Cybercrime: Wenn es dann doch passiert ist – Lösungen der Versicherungsbranche
Unternehmen unterschätzen das Risiko, einer Cybercrime-Attacke zum Opfer zu fallen, nach wie vor. Was Geschäftsleiter und Compliance Officer im Umgang mit Cybercrime beachten sollten und welche Lösungen die Versicherungswirtschaft bietet, erläutert Dominik Baumann.

Recht

designer491/iStock/Thinkstock

„Vor allem der Reputationsschaden ist massiv"
Compliance-Verstöße bei Non-Profit-Organisationen (NPO) haben in jüngster Zeit für starke mediale Aufmerksamkeit gesorgt. Solche Vorfälle und Skandale können für Stiftungen und Vereine existenzgefährdend sein, wie Dr. Rita Pikó in unserem Interview beschreibt.

Die ideale Compliance-Welt

Die Moralisierung des Rechts ist im Aufwind, stellt Dr. Malte Passarge fest und sieht darin mit einer großen Portion Ironie die „ideale Compliance-Welt". Sehr ernst gemeint ist dagegen seine Beschreibung der – auch durch den technologischen Fortschritt getriebenen – Entwicklung hin zum Überwachungssystem für „unethisches Verhalten".

metamorworks/iStock/Thinkstock

Überwachung per Kamera, Gesichtserkennung und Auswertung der Internetaktivitäten: Sie sind der technologische Trumpf der „idealen Compliance-Welt".

Die ideale Compliance-Welt findet man in China! Todesstrafe bei Korruption und ein Überwachungssystem, das den folgsamen Bürger belohnt. Nach dem Social Credit System, das 2020 eingeführt werden soll, wird das Verhalten eines jeden Bürgers bewertet. Kleine Verfehlungen werden nicht mit überzogenen Gefängnisstrafen, sondern mit einem Bürgerwert bestraft – gutes Verhalten belohnt. Zu schnelles Autofahren, bei Rot über die Ampel gehen, zu hohe Schulden, das gibt ein schlechtes Scoring mit der Folge, dass man sich keine Flugtickets kaufen kann, keinen Kredit erhält und Ärger mit den Behörden hat. Gut ist, wer sich regelkonform verhält, Biogemüse kauft und seine Rechnung pünktlich bezahlt. Mit einem hohen Bürger-Rating erhält man günstige Kredite, Vorteile bei der Wohnungsvergabe, Studienplätze für das Kind und eine günstigere Krankenversicherung. Das alles wird durch eine umfassende Überwachung per Kamera, Gesichtserkennung und Auswertung der Internetaktivitäten objektiv erkannt und festgestellt.

Ein nachhaltiges und ergebnisorientiertes Sanktionssystem ohne die Kosten und Mühen eines Prozesses. Der Traum eines jeden Compliance-Officers – so stellt man sich die perfekte Compliance-Welt vor!

Auch in Deutschland haben wir wichtige erste Schritte in diese Richtung erreicht. Wurde zunächst die erste Initiative zum gesetzlich vorgegebenen richtigen Essen noch verlacht (sog. Veggie-Day), geht es nun forsch voran. Derzeit müssen in vielen Fällen noch die Medien und die Öffentlichkeit bemüht werden, um missliebige Personen ohne einen Prozess nachhaltig zu verurteilen und lebenslange Ächtung auszusprechen. Doch der Gesetzgeber schafft hierzu schon professionelle Strukturen. Die Übertragung von staatlichen Kontroll-, Überwachungs- und Sanktionsaufgaben auf den zu kontrollierenden, überwachenden und sanktionierenden Bürger sind kluge erste Schritte in die Welt des Bürger-Scorings. Angefangen mit der Selbstzensur in Gestalt des Netzwerkdurchsetzungsgesetzes geht es weiter mit umfassenden Rechten und Pflichten des Datenschutzbeauftragten, Verdachtsmeldungen bei Geldwäsche und der Selbstanzeigepflicht bei grenzüberschreitenden Steuergestaltungen. Auch sehr gut ist die Idee, bei Compliance-Verstößen eine Pflicht zur Durchführung von internen Ermittlungen zu schaffen, um dann die Untersuchungsergebnisse des Unternehmens von der Staatsanwaltschaft beschlagnahmen zu können. Gekrönt wird dies durch das jüngst beschlossene Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). Dort wird die Offenlegung von Geschäftsgeheimnissen durch Hinweisgeber nicht nur bei der Verletzung wesentlicher Rechte geschützt, sondern auch bei „Aufdeckung […] eines anderen Fehlverhaltens". In der Gesetzesbegründung wird dieses als „unethisches Verhalten" konkretisiert, das nicht notwendigerweise gegen Rechtsvorschriften verstoßen muss. Das gelobte Land ist in Sicht!

Achtung, das war Ironie. Dabei kann einem das Lachen im Halse stecken bleiben. Viele widersprüchliche Tendenzen sind derzeit zu bestaunen, das Verständnis für die Grundstrukturen und Vorzüge eines Rechtsstaates scheint zu schwinden. Die Moralisierung des Rechts, die Individualisierung des Rechts, das göttliche Recht und der Rechtspositivismus sind im Aufwind, zugleich wird die folgenschwere Überlastung des Justizapparates spürbar.

Was bedeutet das alles für den Bereich-Compliance? In der kleinen aber wichtigen Compliance-Welt darf nicht vergessen werden, dass konsequente Regeln und Sanktionen zur Verhinderung von Gesetzesverstößen und Missbrauch gut und richtig sind. Komplexe unternehmerische Strukturen fordern eine komplexere Compliance-Architektur. Dabei dürfen aber der gesunde Menschenverstand und die Verantwortung des Einzelnen nicht vergessen werden. Denn je komplexer Compliance-Strukturen sind, desto größer ist die Gefahr, dass der Einzelne seine Verantwortung an diese Strukturen abgibt. Aktuelle Fälle aus der Welt der Großkonzerne sind warnende Beispiele. Bei allem Streben nach Redlichkeit im Geschäftsverkehr darf nicht übersehen werden, welch hohes Gut Rechtsstaatlichkeit ist und was dies im Tagesgeschäft wirklich bedeutet. Nicht nur der einzelne Bürger und Unternehmen haben dies zu beachten, auch staatliche Institutionen, die Legislative und die Exekutive dürfen das manchmal etwas lästige Gefüge der Rechtsstaatlichkeit nicht unterschätzen. Es darf nicht vergessen werden, dass jeder Mitarbeiter, jeder Compliance-Beauftragte, jeder Unternehmer und jeder Rechtsanwender auch Bürger und für die Gestaltung unseres Landes verantwortlich ist.

Dr. Malte Passarge

privat

Dr. Malte Passarge ist Rechtsanwalt und Fachanwalt für Handels- und Gesellschaftsrecht in der Kanzlei Passarge, Prudentino & Rhein PartGmbB – Studio Legale sowie Vorstand des Instituts für Compliance im Mittelstand (ICM), Geschäftsführer von Pro Honore e. V. und Chefredakteur des Compliance-Beraters.

Diskutieren Sie mit!

Wie sehen Sie die aktuellen Entwicklungen im Licht der Compliance? Wir freuen uns auf eine angeregte und kontroverse Diskussion, auch zu grundlegenden Compliance-Fragen.

Schreiben Sie uns!

Zuschriften an: christina.kahlen-pappas@dfv.de

C.F. MÜLLER COMPLIANCE

Rechtskonform bis ins Detail

Compliance

Aufbau - Management - Risikobereiche

Herausgegeben von Dr. Cornelia Inderst, RAin, Prof. Dr. Britta Bannenberg und Sina Poppe, RAin.
3. Auflage 2017. 856 Seiten. € 139,99
ISBN 978-3-8114-4661-8

Das Grundlagenhandbuch

„Das Buch ist durch eine hohe Praxisorientierung gekennzeichnet und gibt dem interessierten Leser klare Informationen in die Hand, die tatsächlich umsetzbar sind."
Reiner Quick in: Die Wirtschaftsprüfung 9/2014

Tax Compliance

Prävention - Investigation - Remediation - Unternehmensverteidigung

Herausgegeben von Dr. Markus Rübenstahl, Mag.iur., RA, und Dipl.-Kfm. Jesco Idler, WP und StB.
2018. 1.569 Seiten. € 159,99
ISBN 978-3-8114-4657-1

Steuerliche Risiken erkennen und beherrschen

Das Handbuch behandelt die steuerlichen Verfahrensabläufe, Fragestellungen und Probleme mit In- und/oder Auslandsbezug umfassend und abschließend.

Kapitalmarkt Compliance

Herausgegeben von Dr. André-M. Szesny, LL.M., RA, und Dr. Thorsten Kuthe, RA.
2. Auflage 2018.
Ca. 1.500 Seiten. Ca. € 149,99
ISBN 978-3-8114-4659-5
Neu im Oktober

Das Compliance-Handbuch für kapitalmarktorientierte Unternehmen.

Die Änderungen durch die EU-Richtlinie MIFID II und die begleitende EU-Verordnung MIFIR bringen erhebliche regulatorische Änderungenfür kapitalmarktorientierte Unternehmen.
Das Handbuch zeigt die Lösung – topaktuell, auf dem neuesten Stand.

Versandkostenfreie Bestellung und E-Book-Download: www.cfmueller.de

C.F. Müller GmbH, Waldhofer Straße 100, 69123 Heidelberg
Bestell-Tel. 089/2183-7923, Bestell-Fax 089/2183-7620, E-Mail: kundenservice@cfmueller.de

C.F. Müller

Cybercrime: Vom Opfer zum Täter – die Verantwortung des Managements

Chefbetrug bzw. CEO-Fraud ist inzwischen eine bekannte Masche. Trotzdem gelingt es den Betrügern weiterhin, vor allem mittelständische Unternehmen massiv zu schädigen. Für Unternehmen bedeutet diese Entwicklung vor allem eines: Ein Perspektivwechsel ist nötig!

BrianAJackson/iStock/Thinkstock

Cybercrime im Blick: Wer die vielfältigen Bedrohungslagen aus den Augen verliert, verletzt seine Compliance-Pflichten.

Betrugsopfer, gerade im wirtschaftsstrafrechtlichen Kontext, wird man vor allem dann, wenn entweder Gier oder aber Angst das eigene Handeln beeinflusst. Dann sind oft sämtliche mühsam antrainierten Vorsichtsmaßnahmen vergessen und das Unternehmen wird zum Opfer der Betrüger. Trotz dieser „Opferrolle" sollten Unternehmen dringend die Perspektive wechseln. Denn je bekannter die Methodik der Straftäter ist, weil etwa Informationsquellen und Auffrischungs-Seminare zum Thema leicht zugänglich sind, desto näher liegt es, an eine Pflichtverletzung des Managements zu denken, wenn Betrüger das Unternehmen schädigen. Damit wird das Unternehmen zwar nicht zum „Täter", doch wer seine Compliance-Struktur nicht regelmäßig an das reale Bedrohungsszenario anpasst, allgemein bekannte Risiken und deren Auswirkungen auf das eigene Unternehmen nicht analysiert, diese Pflichten nicht wirksam delegiert – das von ihm geführte Unternehmen also nur unzureichend gegen die vielfältigen Bedrohungslagen im Bereich Cybercrime schützt – verletzt seine Compliance-Pflichten.

Der Aufsichtsrat ist dann in der Folge verpflichtet, eine Schadenersatzpflicht der Geschäftsleitung zu prüfen, den Vorgang dazu untersuchen zu lassen und gegebenenfalls Organhaftungsverfahren voranzutreiben. Die Erfahrung zeigt, dass nach einer Schadensmeldung an die D&O- sowie auch die Vertrauensschadenversicherung oft ein sehr intensiver Streit geführt wird, ob die erlebte Opfersituation vorhersehbar und vermeidbar gewesen wäre. Das trifft zunächst die Führungskräfte, die sich mehr denn je rechtfertigen müssen, weshalb sie in einem bekanntermaßen gefährdeten Umfeld genügende Schutzmaßnahmen mit Blick auf das von ihnen zu betreuende Unternehmensvermögen unterlassen haben. Damit könnte auch das Unternehmen selbst nach einer so genannten Anordnung der Nebenbeteiligung in den Fokus rücken. Mit Blick auf das ordnungswidrigkeitenrechtliche Regime aus Verbandsgeldbuße und Verletzung der Aufsichtspflicht sowie Untreue durch Unterlassen als Anknüpfungstat ist das eine rechtlich interessante und praktisch durchaus kostspielige Entwicklung.

Zu denken wäre schließlich – im Falle regulierter Industrien – auch an durch die jeweils zuständige Aufsichtsbehörde veranlasste Konsequenzen personeller Natur: Ob deren Feststellungen zu einem mangelhaften Internen Kontrollsystem zur Vermeidung sonstiger Straftaten zu Veränderungen innerhalb der Compliance-Funktion oder der zweiten Führungsebene führen, interessiert in der Praxis kaum. Zentrale Frage wird etwa bei sich anschließenden Haupt-, Gesellschafter- oder Vertreterversammlungen sein, weshalb es der Vorstand oder die Geschäftsführung so weit hat kommen lassen.

Jörg Bielefeld

BEITEN BURKHARDT

Jörg Bielefeld ist Rechtsanwalt und Partner bei BEITEN BURKHARDT in Frankfurt und München. Er leitet den Bereich Wirtschaftsstrafrecht und Compliance.

Compliance beginnt beim Management

Anhand des Beispiels „Cybercrime" zeigt sich einmal mehr, dass jedes Management zu jeder Zeit „harte" Antworten auf folgende Fragen liefern oder zumindest ableiten können sollte:

1. Wie sind wir bezüglich des Schutzes vor Cybercrime organisiert und wie sehen die tatsächlichen Betriebsabläufe aus?
2. Wie sind unsere Verantwortlichkeiten in den einzelnen relevanten Bereichen abgegrenzt?
3. Welche internen Anweisungen gibt es, nach denen Pflichten, gegen die verstoßen werden könnte, an Mitarbeiter delegiert worden sind?
4. Welche Organisations-, Kontroll- und Aufsichtsmaßnahmen haben wir getroffen, damit solche Pflichtenverstöße verhindert oder erschwert werden?
5. Wie haben wir all das dokumentiert?
6. Welchen Eindruck hätten Dritte (etwa Behörden, aber auch Rechtsanwälte) bei einer Überprüfung?
7. Was würden Mitarbeiter, so sie dazu befragt werden, über unsere Schutzmechanismen und Sensibilisierungsmaßnahmen sagen?

Mehr zu Cybercrime erfahren Sie am 22.10.2018 in Frankfurt a.M. beim **Roundtable Cybercrime**. Der zweieinhalbstündige Roundtable (17 bis 19.30 Uhr) zeigt auf, wie sich (mittelständische) Unternehmen gegen Hackerangriffe wappnen können.

Welche Maßnahmen zielführend sind und was man tun kann, wenn das eigene Unternehmen Opfer einer Cybercrime-Attacke wurde, erläutern Stefan Becker, Referatsleiter, Bundesamt für Sicherheit in der Informationstechnik (BSI), Jörg Bielefeld, Partner, BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH, und Peter Zawilla, Geschäftsführer, FMS Fraud & Compliance Management Services GmbH.

Weitere Infos und Anmeldung:
Sonja.Poertner@dfv.de

Cybercrime: Wenn es dann doch passiert ist – Lösungen der Versicherungsbranche

Unternehmen unterschätzen das Risiko, einer Cybercrime-Attacke zum Opfer zu fallen, nach wie vor. Was Geschäftsleiter und Compliance Officer im Umgang mit Cybercrime beachten sollten und welche Lösungen die Versicherungswirtschaft bietet, erläutert Dominik Baumann.

Das Bundeskriminalamt unterscheidet in dem jährlich erscheinenden Bundeslagebild Cybercrime zwischen Cybercrime im engeren Sinne und Straftaten, die mittels Informationstechnik begangen werden. Unter Cybercrime im engeren Sinne fallen Straftaten, die sich gegen das Internet, Datennetze, IT-Systeme oder deren Daten richten. Also Straftaten, die gemeinhin als Hackerangriff oder Viren-Attacke bezeichnet werden. Ist die IT im Unternehmen durch Firewall und Viren-Scanner nicht richtig geschützt, erlangen Kriminelle schnell Zugriff auf Geschäftsgeheimnisse und persönliche Daten von Mitarbeitern, Geschäftspartnern sowie Kunden.

Wenn aber E-Mails zum Tatmittel werden, die Informationstechnik also nicht angegriffen, sondern zur Begehung der Straftat genutzt wird, dann hilft auch die vermeintlich sicherste IT-Infrastruktur nicht mehr, einen Vermögensschaden vom Unternehmen abzuwenden. Alle Modi Operandi des Betrugs mittels E-Mail haben dabei eines gemeinsam: sie täuschen über Identitäten und nutzen so die Schwachstelle Mensch aus.

Betrugsszenarien, die als CEO- oder Fake-President-Fraud, Payment-Diversion-Fraud oder Fake-Identity-Fraud bezeichnet werden, haben in der Wirtschaft zwischenzeitlich traurige Berühmtheit erlangt. Ein ausgefeiltes Social Engineering und der steigende Druck auf Mitarbeiter in der heutigen Arbeitswelt lassen immer neue Betrugsmaschen entstehen. Funktioniert die eine Masche nicht mehr, um Mitarbeiter zur Transaktion hoher Geldbeträge zu bewegen, wird schnellstens eine neue Tatvariante von der organisierten Kriminalität entwickelt.

Die immer neuen Betrugsvarianten zeitnah zu erkennen, zu melden und im Unternehmen bekannt zu machen, ist kaum möglich. Ein funktionierendes Compliance-Management kann aber dazu beitragen, dass Betrügereien besser erkannt und Schäden verhütet werden. Wird Compliance im Unternehmen gelebt und eine offene Unternehmenskultur gefördert, haben es Täter deutlich schwerer, psychologischen Druck auf Mitarbeiter auszuüben. Mitarbeiter müssen sicher sein können, dass sie keine Sanktionen zu befürchten haben, wenn sie beim Chef persönlich nachfragen, ob ein bestimmter Geldtransfer tatsächlich gewollt sei.

aurielaki/iStock/Thinkstock

Cybercrime: Was tun, wenn Betrüger zugeschlagen haben?

Durch eine transparente Kommunikation auf allen Ebenen, die Sensibilisierung der Mitarbeiter durch regelmäßige Information und Schulung zu einem drohenden Identitätsbetrug mittels E-Mail und die Implementierung eines unumstößlichen Vier-Augen-Prinzips oder einer Zwei-Unterschriften-Anforderung bei Überweisungen kann ein Unternehmen vorbeugen. Ganz zu verhindern wird es jedoch nicht sein, dass Betrüger illegal erbeutete Informationen dazu verwenden, Menschen zu einem bestimmten Verhalten zu bewegen. Das zeigen die zahlreichen Schadenfälle, die in der Bundeskriminalstatistik ausgewiesen, in den Medien bekannt und bei Versicherungen angezeigt werden.

Versagt der Schutz durch IT-Sicherheit und Compliance-Management, bietet die Versicherungswirtschaft Lösungen an, um Unternehmen im Falle von Cybercrime handlungsfähig und liquide zu halten. Neuartige Cyber-Risk-Policen bieten unter anderem Assistence-Leistungen wie 24/7-Hotlines zu IT-Dienstleistern, die Computersysteme in kurzer Zeit von einem Virenbefall befreien und den Betrieb wieder zum Laufen bringen. D&O-Versicherungen schützen Manager, wenn sie sich dem Vorwurf ihres Unternehmens ausgesetzt sehen, ein Betrugsschaden sei durch die unterlassene Einführung oder nicht wirksame Umsetzung eines Compliance-Management-Systems entstanden. Ziel sollte aber sein, den Schutz der D&O-Versicherung in einem solchen Falle nicht in Anspruch nehmen zu müssen und den originär durch den Betrug entstandenen Vermögensschaden ersetzt zu bekommen.

In diesem und allen anderen Fällen, in denen Unternehmen Schäden durch kriminelle Handlungen von außenstehenden Dritten oder Mitarbeitern erleiden, greift die Vertrauensschadenversicherung. Ist der Betrug erfolgreich gewesen und kann das überwiesene Geld nicht mehr zurückgeholt werden, erhält das Unternehmen nicht nur den Geldbetrag ersetzt, sondern unter anderem auch alle Kosten, die im Zusammenhang mit der Aufarbeitung des Schadeneintritts sowie der Rechtsverfolgung entstehen.

Dominik Baumann


R+V

Dominik Baumann ist Key Account Manager und Underwriter Vertrauensschadenversicherung bei der R+V Allgemeine Versicherung AG mit Sitz in Wiesbaden. Seit über sieben Jahren beschäftigt sich der Volljurist mit Versicherungskonzepten, die Unternehmen bei Schäden durch kriminelle Handlungen Schutz bieten.

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. 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
Verlagsleitung: RA Torsten Kutschke, Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Lena Moneck,Telefon: 069 7595-2713, E-Mail: lena.moneck@dfv.de
Mitherausgeber:
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe AG; Ralf Brandt, divieni patch Beteiligungs GmbH; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; 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, Getzner Textil AG; 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.de

Compliance Berater | Betriebs Berater | Compliance – Die Zeitschrift für Compliance-Verantwortliche | Compliance & Finance – Die Zeitschrift für Compliance in der Finanzbranche

Praxisseminar zum neuen Geldwäschegesetz

11. September 2018 – Frankfurt am Main

September 2018

Mo	Di	Mi	Do	Fr	Sa	So
					1	2
3	4	5	6	7	8	9
10	**11**	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Praxisseminar zum neuen Geldwäschegesetz

Veranstaltungsort:
Gleiss Lutz
Taunusanlage 11
60329 Frankfurt am Main

Teilnahmegebühr:

Abonnenten CB/BB und Übersendung des Kaufbelegs des Kommentars GwG, Zentes/Glaab	699,-€
Bei Übersendung des Kaufbelegs des Kommentars GwG, Zentes/Glaab	749,-€
Abonnenten CB/BB	799,-€
Teilnahmegebühr, regulär	899,-€

Früh-/Mehrbucherrabatt:
Frühbucherrabatt 5% bei Buchung bis 27. Juli 2018, Mehrbucherrabatt 5% bei Anmeldung von mehr als 2 Teilnehmern einer Kanzlei/eines Unternehmens ab dem 3. Teilnehmer (unabhängig vom Frühbucherrabatt)

Anmeldeschluss: 7. September 2018
Eine frühzeitige Anmeldung wird empfohlen.

Anmeldung:
Herrn Torsten Kutschke
Deutscher Fachverlag GmbH
Mainzer Landstraße 251, 60326 Frankfurt am Main
Telefon: 069/7595-1151, E-Mail: Torsten.Kutschke@dfv.de

Stornierung:
Die Anmeldung ist übertragbar. Bei Stornierung bis zum 24. August 2018 wird eine Bearbeitungsgebühr in Höhe von 50,-€ erhoben.Danach und bei Nichterscheinen eines Teilnehmers ist die volle Teilnahmegebühr zu entrichten.

Der Preis schließt Veranstaltungsunterlagen und die Pausenverpflegung mit ein.
Die Teilnahmegebühr bitten wir erst nach Erhalt der Rechnung zu überweisen.
Eine Teilnahmebestätigung nach § 15 FAO wird erteilt.

Anmeldung Praxisseminar zum neuen Geldwäschegesetz am 11. September 2018

per Fax an: 069/75951150

Kanzlei / Firma: _____

Name, Vorname: _____

Straße, Nr.: _____

PLZ, Ort: _____

Tel.: _____ E-Mail: _____

Datum: _____ Unterschrift: _____

- ❑ Teilnehmer, regulär
- ❑ Abonnent CB/BB
- ❑ Kaufbeleg Kommentar GwG, Zentes/Glaab
- ❑ Abonnent CB/BB und Kaufbeleg Kommentar GwG, Zentes/Glaab

GwG-Kommentar, Zentes/Glaab
❑ Bitte senden Sie mir den neuen Kommentar zum GwG von Zentes/Glaab für 219,-€ zu.

„Vor allem der Reputationsschaden ist massiv“

Compliance-Verstöße bei Non-Profit-Organisationen (NPO) haben in jüngster Zeit für starke mediale Aufmerksamkeit gesorgt. Solche Vorfälle und Skandale können für Stiftungen und Vereine existenzgefährdend sein. Trotzdem scheuen gerade kleinere und mittlere NPOs vor der Implementierung von Compliance-Management-Systemen (CMS) zurück, weil sie den Aufwand als unverhältnismäßig empfinden. Welche Konsequenzen das haben kann und wie ein verhältnismäßiges und zweckdienliches CMS für NPOs ausgestaltet sein sollte, erklärt in unserem Interview Dr. Rita Pikó.

designer491/iStock/Thinkstock

Non-Profit-Organisationen: Sie stehen bei Compliance-Verstößen besonders im Fokus der Öffentlichkeit.

» Warum können gerade für NPOs Compliance-Vorfälle gravierende Folgen haben?

« Eine NPO kann durch einen Compliance-Vorfall auf unterschiedlichen Ebenen betroffen sein. Vor allem der Reputationsschaden ist für gemeinnützige Organisationen massiv. Der Vorfall kann aber auch den Entzug der Gemeinnützigkeit bzw. Straf- oder Ordnungswidrigkeits- und Schadenersatzverfahren nach sich ziehen. Schließlich kann ein Compliance-Vorfall zum Weggang von tragenden Funktionsträgern führen. Neue Mitarbeiter für Schlüsselfunktionen sind dann schwer zu finden.

NPOs in der Kritik

Anfang des Jahres wurden mehrere Missbrauchsfälle Schutzbedürftiger durch Führungskräfte und Mitarbeiter der Hilfsorganisation Oxfam auf Haiti bekannt. Die Ereignisse beherrschten über Wochen insbesondere die Medien in Großbritannien. Unter dem Schlagwort #AidToo formierte sich – parallel zur #MeToo-Bewegung – eine intensiv geführte Debatte. Dabei reiht sich der Oxfam-Fall in vergleichbare Fälle sexueller Übergriffe und Machtmissbrauch durch Mitarbeiter karitativer Organisationen ein, wie die des Schweizer Vereins Save the Children oder des deutschen Vereins Weißer Ring. Bei Oxfam trat in kürzester Zeit ein bisher nie dagewesener Reputationsverlust ein, einhergehend mit dem Vertrauensverlust der Spender. Binnen zehn Tagen verlor die Organisation 7.000 Spender, die britische und die Schweizer Regierungen zahlen derzeit keine weiteren Gelder an Oxfam. Die Hilfsorganisation musste ihre Arbeit in Haiti für zwei Monate aussetzen, ihr Präsident hat seinen Rücktritt angekündigt, ihre Vize-Präsidentin trat zurück, Mitarbeiter wurden entlassen.

» Sie raten dazu, dass NPOs sich präventiv vor Compliance-Verstößen schützen. Wie sollten sie hierbei vorgehen?

« Der erste Schritt sollte die Analyse der potentiellen Compliance-Risiken sein: also eine Compliance-Risikoanalyse (CRA). Compliance-Risiken folgen aus der – potentiellen – Verletzung von sanktionsbewehrten Gesetzesvorschriften. Die NPO kann auch eigene Regularien darunter fassen und ihre internen Richtlinien, wie z. B. ihren Verhaltenskodex, dazuzählen. Es ist ratsam, zunächst die Ist-Situation zu analysieren und eine strategische Bestandsaufnahme zu erstellen. Wurden bereits Regeln in den identifizierten Risikobereichen aufgestellt? Wer ist für welche Risiken zuständig? Wurden die Prozesse bereits festgelegt? Gab es in der Vergangenheit schon Compliance-Verstöße?

» Auf welche Besonderheiten sollte eine NPO sich bei dieser Compliance-Risikoanalyse einstellen?

« Besondere Risikofelder für NPOs sind Interessenkonflikte, Aberkennung der Gemeinnützigkeit, Korruption im In- und Ausland sowie Geldwäsche und Terrorismusfinanzierung. Um Interessenkonflikte von vorneherein zu vermeiden, müssen Gremiumsmitglieder ihre potentiellen Interessenkollisionen offenlegen. Die Aberkennung der Gemeinnützigkeit kann die NPO treffen, wenn zum Beispiel Zahlungen für Gefälligkeiten aus dem Stiftungsvermögen erfolgen oder Spenden für private Zwecke verwendet werden. Das kann eine Veruntreuung des Stiftungsvermögens darstellen. Das höchste Korruptionsrisiko besteht bei den internationalen Stiftungen, da diese vielfach in Krisengebieten und Regionen tätig sind, in denen eine hohe Korruption herrscht. Zudem haben international durchgeführte Analysen der Geldströme im Zusammenhang mit terroristischen Anschlägen Fälle aufgedeckt, bei denen NPOs für Terrorismusfinanzierung missbraucht wurden.

» Wie sollte ein Compliance-Management-System für NPOs ausgestaltet sein?

« Die Ausgestaltung hängt maßgeblich von der Größe der NPO, dem Umsatz, der Organisationsstruktur, dem Tätigkeitsfeld, der geografischen Präsenz und den Ergebnissen der CRA ab. Das zentrale Werkzeug zur Vermittlung der Compliance-Kultur ist der Verhaltenskodex. Die nachhaltigsten Elemente eines CMS sind Schulungen. Sie sollten auf allen Hierarchieebenen durchgeführt werden, damit Organmitglieder wie Beschäftigte für Compliance-relevante Themen sensibilisiert sind. Aber auch die Implementierung eines Hinweisgebersystems gehört zu einem CMS, um Beschäftigten die Möglichkeit einzuräumen, geschützt Hinweise auf Compliance-Verstöße in ihrer NPO zu geben.

chk

Foto Dr. Rita Pikó

Dr. Rita Pikó, LL.M. (Exeter), ist Dozentin an der Zürcher Hochschule für Angewandte Wissenschaften und Studiengangleiterin des CAS Compliance Investigator sowie Rechtsanwältin in Zürich.

Mehr zu Compliance bei Non-Profit-Organisationen lesen Sie in den ausführlichen Beiträgen von Dr. Rita Pikó im **Compliance-Berater**, Ausgabe 7/2018 und 8/2018.

Compliance
Die Zeitschrift für Compliance-Verantwortliche

Roundtable Cybercrime

Schutz | Abwehr | Schadensbegrenzung

22 . Oktober 2018 – Frankfurt am Main

Oktober 2018

Mo	Di	Mi	Do	Fr	Sa	So
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Roundtable Cybercrime

Referenten:

Stefan Becker, Referatsleiter, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Jörg Bielefeld, Partner, BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH

Peter Zawilla, Geschäftsführer, FMS Fraud & Compliance Management Services GmbH

Veranstaltungsort:
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Mainzer Landstraße 36 • 60325 Frankfurt am Main

Programm:
16.30 Uhr Registrierung der Teilnehmer
17.00 Uhr Beginn des Roundtable
- Cybercrime: Was muss ich jetzt wissen?
- Wie können sich (mittelständische) Unternehmen gegen Hackerangriffe wappnen?
- Cybersecurity: Welche Maßnahmen sind zielführend?
- Was kann man tun, wenn das eigene Unternehmen Opfer einer Cybercrime-Attacke wurde?

19.30 Uhr Get-together

Teilnahmegebühr: 69,- €

Anmeldeschluss: 18. Oktober 2018
Eine frühzeitige Anmeldung wird empfohlen.

Anmeldung:
Frau Sonja Pörtner
Deutscher Fachverlag GmbH
Mainzer Landstraße 251 • 60326 Frankfurt am Main
Telefon: 069/7595-1163 • E-Mail: Sonja.Poertner@dfv.de

Stornierung:
Die Anmeldung ist übertragbar. Bei Stornierung bis zum 1. Oktober 2018 wird eine Bearbeitungsgebühr in Höhe von 50,-€ erhoben. Danach und bei Nichterscheinen eines Teilnehmers ist die volle Teilnahmegebühr zu entrichten.

Der Preis schließt die Pausenverpflegung mit ein.
Die Teilnahmegebühr bitten wir erst nach Erhalt der Rechnung zu überweisen.
Eine Teilnahmebestätigung nach § 15 FAO wird erteilt.

Anmeldung Roundtable Cybercrime

Kanzlei / Firma: _____

Name, Vorname: _____

Straße, Nr.: _____

PLZ, Ort: _____

Tel.: _____ E-Mail: _____

Datum: _____ Unterschrift: _____

Programm:
www.compliance-plattform.de

per Fax an: 069/7595-1150

❑ Ja, ich nehme am Roundtable Cybercrime teil.
❑ Ja, ich nehmen am Get-together im Anschluss an die Veranstaltung teil.