Compliance
Die Zeitschrift für Compliance-Verantwortliche

Juli 2017

Inhalt

Aufmacher

DFB setzt auf integratives CMS

Zur Vorabendveranstaltung der Deutschen Compliance Konferenz 2017 lud am 27. Juni der Deutsche Fußball-Bund in seine Zentralverwaltung nach Frankfurt ein. In einem Auftaktvortrag zum Thema „Perspektiven des Compliance-Managements im Sport" erläuterte Dr. Ulrich Bergmoser das neue Compliance-Management-System des DFB und nutzte die Gelegenheit, Missverständnisse über den DFB und Compliance im Sport auszuräumen.

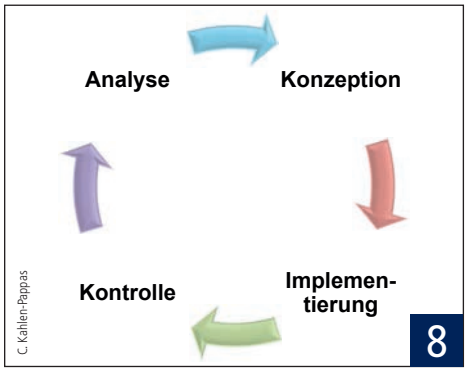
Veranstaltung

Deutsche Compliance Konferenz 2017
„Compliance der Zukunft" – was ist neu und was kommt in nächster Zeit noch auf Unternehmen, Vereine und deren Compliance-Verantwortliche zu? Darüber diskutierten anlässlich der Deutschen Compliance Konferenz 2017 Juristen und Praktiker.

Praxis

Messbarkeit von Compliance-Maßnahmen
Nur was gemessen werden kann, lässt sich auch steuern – also effizienter und effektiver gestalten. Ob und wie das auch für Compliance gelten kann, erklärt Michael Kayser in unserem Interview.

Praxis



In vier Schritten zur Corporate Compliance
Nikolai Unmuth erkärt, wie ein auf den Einzelfall abgestimmtes Compliance-System in vier Schritten aufgebaut werden kann.

News

International

DFB setzt auf integratives CMS

Zur Vorabendveranstaltung der Deutschen Compliance Konferenz 2017 lud am 27. Juni der Deutsche Fußball-Bund in seine Zentralverwaltung nach Frankfurt ein. In einem Auftaktvortrag zum Thema „Perspektiven des Compliance-Managements im Sport" erläuterte Dr. Ulrich Bergmoser das neue Compliance-Management-System des DFB und nutzte die Gelegenheit, Missverständnisse über den DFB und Compliance im Sport auszuräumen.

Vorabendempfang zur Deutschen Compliance Konferenz 2017 in der DFB-Zentrale.

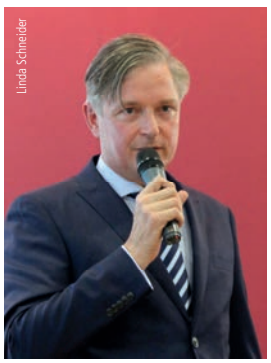
Compliance und Sport – das ist offenbar eine interessante und schwierige Kombination. Aber auch eine Kombination, die – zumindest in Bezug auf den Deutschen Fußball-Bund – gewissen Missverständnissen in der Öffentlichkeit ausgesetzt sei, betonte Dr. Ulrich Bergmoser, DFB-Direktor Finanzen, IT, Personalwesen und Zentrale Dienste.

Ein wesentliches Missverständnis sei, dass der DFB mit seinem Compliance-Programm nur auf die Berichterstattung der jüngsten Vergangenheit reagiere: „Fußball ist eine hoch emotionale Industrie, in der auch Compliance eine wichtige Rolle spielt. Aber das nicht erst, seit die WM-Affäre ans Licht kam." Bereits 2012 hatte der DFB einen Verhaltenskodex eingeführt, der für alle Mitarbeiter im Hauptamt verpflichtend ist. 2014 erfolgte dann eine erste Analyse der Compliance-Risiken durch einen unabhängigen Sachverständigen. Der Beschluss, ein Compliance-Management-System einzuführen, fiel im DFB-Präsidium 2015 – also in dem Jahr als die „WM-Affäre" aufgedeckt wurde.

Seither schreite die Einführung des CMS voran, berichtet Bergmoser und räumt selbstkritisch ein: „Wir sind immer noch nicht so schnell, wie wir sein sollten, aber wir sind schneller als alle anderen, die in der Branche unterwegs sind." Ein Grund für das Tempo, mit dem Compliance den DFB durchdringt, sei auch seine Struktur und Größe. „Der DFB", so Bergmoser, „ist der größte Sportverband der Welt, der an der Spitze von fünf Regionalverbänden, 21 Landesverbänden und mehr als 25.000 Vereinen deutschlandweit steht." Dies sei „ein ganz besonderer Kontext für Compliance, in dem vielfältige Interessen miteinander in Einklang zu bringen sind."

Eine erhebliche Herausforderung dabei: die Kommerzialisierung des Sports. Denn „unsere Möglichkeiten zur Förderung des Breitensports und auch dessen soziale Funktion haben natürlich ihre Grundlage in der Kommerzialisierung", stellt Bergmoser klar. Eine Grundherausforderung des DFB aus Governance-Perspektive bestehe darin, dass er immer noch als Verein aufgestellt ist. „Diese Rechtsform ist für ein Konstrukt mit 300 Mio. Euro Umsatz eigentlich nicht gemacht." Dass nicht nur die Finanzbehörden sondern vor allem auch die Öffentlichkeit den DFB hierbei kritisch beobachte, sei ganz natürlich und richtig: „Wir sind Vorbild und stellen uns unserer gesellschaftlichen Verantwortung." Für den DFB bedeute das, Rechenschaft abzulegen, denn diese sei die Kehrseite der Verantwortung. Rechenschaft wiederum setze Transparenz voraus.

Ausgerichtet am IDW PS 980 baue der DFB ein „integratives Compliance-System" mit vier Kernprozessen auf: der zyklischen Risikoinventur, Berichterstattung und Überwachung, der Aus- und Fortbildung sowie der Überprüfung der Angemessenheit der Regelwerke des DFB.



Dr. Ulrich Bergmoser, DFB-Direktor Finanzen, IT, Personalwesen und Zentrale Dienste

Wichtig ist Bergmoser dabei vor allem, dass Compliance sich nicht in dem Erlass von Richtlinien und Regelungen erschöpft, sondern in die bestehenden Prozesse und Arbeitsabläufe integriert wird: „Compliance ist eine kulturelle Aufgabe, die alle angeht. Dies allein einer speziellen Abteilung zu übertragen, wäre der falsche Ansatz." Im DFB hat daher die Revision die zentrale Kontrollfunktion auch für Compliance übernommen. „Unser CMS braucht ein unabhängiges Element, auf das die Leitung keinen Einfluss hat. So ein Element ist die Revision. Und die müssen wir mit der Fähigkeit ausstatten, Compliance zu untersuchen." Um die vier Kernprozesse des CMS „am Laufen zu halten", hat der DFB weitere Verantwortlichkeiten an die bereits bestehenden Funktionen Controlling, Human Resources und Recht verteilt. Die Koordination der vier Prozesse übernehme der Compliance-Verantwortliche.

Für Bergmoser ist klar, dass die „Road to Compliance" mit der Einrichtung des CMS nicht aufhört: „Wir werden einiges in der Organisation zu optimieren haben, um Verfehlungen von vorneherein zu vermeiden." Doch dabei sehe sich der DFB in guter Gesellschaft mit anderen Unternehmen und Vereinen, die sich zu Compliance bekennen. Und so beschließt Bergmoser seinen Vortrag auch mit einem Praxis-Tipp für alle Compliance-Verantwortlichen unter den Gästen der Vorabendveranstaltung: „Legen Sie Ihren Fokus auf Vertrieb, Leitung und Einkauf – hier stecken die größten Risiken." *chk*

Deutsche Compliance Konferenz 2017

„Compliance der Zukunft" – was ist neu und was kommt in nächster Zeit noch auf Unternehmen, Vereine und deren Compliance-Verantwortliche zu? Darüber diskutierten anlässlich der Deutschen Compliance Konferenz 2017 Juristen und Praktiker.

Sven Jacobs erläuterte den Handlungsrahmen der IT-Compliance.

Dr. Tobias Schwartz erklärte, wie sich das steuerstrafrechtliche Risiko durch Tax. Compliance reduzieren lässt.

Geldwäscherisiken standen im Mittelpunkt des Vortrags von Dr. Dirk Scherp.

Carsten Beisheim befasste sich mit CSR-Compliance.

Dietmar Böhlke (Mitte) gab Einblicke in die Vorbereitungen zur DSGVO bei der Media-Saturn-Holding GmbH. Armin Fladung erläuterte die Perspektiven der DSGVO.

Die Themenschwerpunkte der im Deutschen Fachverlag in Frankfurt ausgerichteten Konferenz reichten von CSR-Compliance und Compliance-Risikomanagement über Datenschutz und IT-Compliance bis hin zu Tax- und Kartellrechts-Compliance. Alle Referenten stellten den direkten Bezug zur Praxis her. Unmittelbar aus ihrer eigenen praktischen Erfahrung in ihrem jeweiligen Unternehmen berichteten Dietmar Böhlke, Media-Saturn-Holding GmbH, Dr. Oliver Mross, Hella KGaA Hueck & Co., sowie Roy Walsh, GfK SE. Lesen Sie in den kommenden Ausgaben von Compliance und in unserer Fachzeitschrift Compliance-Berater ausführliche Beiträge zu den jeweiligen Vorträgen. *chk*

Praxiseinblicke in die Kartellrechts-Compliance bei der Hella KGaA Hueck & Co. gewährte Dr. Oliver Mross. Prof. Dr. Daniela Seeliger berichtete über die jüngsten Veränderungen im Kartellrecht.

Zu Criminal Compliance moderierte Prof. Dr. Martin Schulz (re.) die Diskussion mit Dr. Manfred Rack (Mitte) und Dr. Dirk Scherp (li.).

Dr. Marcus Böttger erläuterte, wann der Staat auf interne Compliance-Unterlagen zugreifen kann.

Compliance & Finance geht an den Start

Unsere Online-Zeitschrift Compliance hat seit Juli eine Schwester: Compliance & Finance.

Seit Anfang Juli hat die dfv Mediengruppe ihr Angebot um eine weitere Online-Zeitschrift zum Thema Compliance ergänzt. Compliance & Finance richtet sich als zentrale Informations- und Kommunikationsplattform an alle Compliance-Verantwortlichen in Banken und Versicherungen aber auch an externe Rechtsanwälte und Berater.

Zentrale Inhalte von Compliance & Finance sind Auf- und Ausbau einer Compliance-Struktur in Banken und Versicherungen, Best-Practice-Beispiele, Informationen zu rechtlichen Neuerungen, Karriere- und Entwicklungschancen, nationale und internationale Compliance-Nachrichten.

In der aktuellen Juli-Ausgabe greift Vanessa Engel, Fachanwältin für Versicherungsrecht und Leiterin des Arbeitskreises Versicherungsrecht im Wiesbadener Anwalt und Notarverein e.V. (WANV) erneut das BGH-Urteil zur Schadensregulierung durch den Versicherungsmakler auf. In ihrem Beitrag erläutert sie, welche Konsequenzen aus den jüngsten Einlassungen der BaFin zum Urteil für die bisherige Praxis der Versicherer und Makler folgen.

Compliance & Finance verschafft jeden Monat einen aktuellen und kurzweiligen Überblick zu Compliance in Banken und Versicherungen.

Außerdem erwartet Sie ein Interview mit Ramon Schürer, der das Thema „Anti-Fraud & Investigations – Advisory" für die Region Deutschland in der Deutschen Bank AG verantwortet. Er beschreibt, wie wirksames Anti-Fraud-Management funktionieren kann, welche Rolle Hinweisgebersysteme spielen und auf welche Veränderungen sich die Finanzbranche mittelfristig einstellen sollte.

Freuen Sie sich auch auf die August-Ausgabe von Compliance & Finance, in der wir uns intensiv mit dem Thema Geldwäsche befassen werden.

Als Abonnent von „Compliance" haben Sie hier die Möglichkeit, sich ab sofort für den regelmäßigen kostenfreien Bezug von „Compliance & Finance" anzumelden. Ich wünsche Ihnen viel Spaß bei der Lektüre! *Christina Kahlen-Pappas*

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
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 Rechtsanwaltsgesellschaft mbH,
KPMG AG, SAI Global
Fachbeirat der Online-Zeitschrift Compliance: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe AG; Ralf Brandt, divieni patch Beteiligungs GmbH; 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

Messbarkeit von Compliance-Maßnahmen

Seit Jahren investieren Unternehmen in Compliance-Management-Systeme. Doch mit welchem Erfolg? Im Unternehmensalltag gilt allgemein: Nur was gemessen werden kann, lässt sich auch steuern – also effizienter und effektiver gestalten. Ob und wie das auch für Compliance gelten kann, erklärt Michael Kayser in unserem Interview.


csj302/iStock/Thinkstock

Compliance unter der Lupe: Der Erfolg der Maßnahmen ist durchaus messbar.

» Die Messbarkeit von Compliance erscheint auf den ersten Blick schwierig. Denn im besten Fall bewirkt ein Compliance-Management-System (CMS), dass es zu keinen Vorfällen kommt. Gibt es also auch nichts zu messen, wenn nichts passiert?

« Der Maßstab, nach dem ein CMS maßgeblich bewertet wird, ist dessen Effektivität. Dies findet sich in oft zitierten Guidelines wie zum Beispiel im Zusammenhang mit dem FCPA oder auch dem UK Bribery Act. Die Effektivität ist auch Gegenstand der Prüfung seitens der Strafverfolgungsbehörden bei Verstößen. Es geht also darum, ob das CMS wirksam ist. Bei dieser Beurteilung spielen selbstverständlich die Anzahl der Hinweise sowie der Umgang mit Verstößen zu Daten, die man messen kann, eine Rolle.

Darüber hinaus gibt es aber weitere Kennzahlen und Daten, die auch ohne Compliance-Fälle Rückschlüsse auf die Wirksamkeit des CMS zulassen können. Hierzu gehört beispielsweise die Anzahl von Meldungen, Anfragen und Hinweisen, die über eine Whistleblowing-Hotline abgegeben werden. Ebenso ist die Nutzung eines Geschenkeregisters ein Anhaltspunkt dafür, ob entsprechende Maßnahmen umgesetzt und gelebt werden.

» Welche Daten eignen sich außerdem für Erhebungen über den Erfolg des unternehmensinternen CMS?

« Zunächst gibt es im Rahmen der Messung des CMS der Organisation die klassischen, objektiven Daten. Hierzu gehören zum Beispiel wie oft eine entsprechende Richtlinie heruntergeladen oder angesehen wurde. Auch lässt sich erheben, wieviele Mitarbeiter in welchem Zeitraum zu bestimmten Themen geschult wurden. Ebenso kann die Nutzung von Hotlines oder Whistleblowing-Arrangements ein Indikator sein.

Interessanter wird es, wenn im Rahmen von Mitarbeiterbefragungen beispielsweise Feedback darüber gesucht wird, ob einerseits die Struktur, Organisation sowie Maßnahmen bekannt sind. Und dem gegenüber gestellt entsprechendes Verhalten beobachtet werden kann. Gerade mit solchen Instrumenten kann die Compliance-Funktion sehr gezielt Verbesserungsbedarf ermitteln, Schwachstellen erkennen, und das CMS gegebenenfalls stärken.

Eine weitere Informationsquelle sind Kennzahlen aus den operativen Prozessen, wie sie zum Beispiel bei der Lieferantenbewertung, entsprechenden Due-Diligence Prozessen anfallen. Hier ließe sich zum Beispiel der Ablehnungsgrad von Lieferanten bewerten. Ebenso vorstellbar ist eine Kennzahl, die aus Compliance-Gründen abgelehnte Geschäfte ermittelt.

» Wie kann ein Unternehmen verifizieren, ob zum Beispiel ein Mitarbeiter-Training die Compliance im Unternehmen erhöht?

« Generell erhöhen Training und Kommunikation das Bewusstsein für Compliance. Ob dies in Verhaltensänderung mündet, hängt nicht nur von der Qualität der Maßnahme ab, sondern auch von der Gesamtheit des CMS. Man kann konkret messen, ob beispielsweise nach einer Sensibilisierungskampagne oder einem Training die Anzahl der Anfragen an die Compliance-Funktion steigen. Dies wäre ein Beleg für ein erhöhtes Interesse am Thema. Ebenso kann man beobachten, inwieweit sich Verhalten ändert, zum Beispiel der Grad zu dem eine Clean-Desk-Policy als Folge eines Trainings zur Informationssicherheit umgesetzt wird.

» Welche Rolle spielen die ISO Standards 19600 und 37001 für die Messbarkeit von Compliance?

« Beide ISO Standards sind Managementsystem-Standards. Eines der wesentlichen Prinzipien dieser Standards ist das Plan-Do-Check-Act-Prinzip der kontinuierlichen Verbesserung. Einfach gesagt, erfordern bzw. empfehlen beide Standards, das Managementsystem zu bewerten und entsprechend anzupassen (Check/Act). Eine Bewertung der Wirksamkeit ist also impliziert. Eine Rolle spielt hier ebenfalls, ob das CMS noch den organisatorischen Anforderungen entspricht oder angepasst werden muss. Es geht also auch um das Umfeld, die regelmäßige Berücksichtigung und Bewertung bestehender oder neu hinzugekommener Risiken etc. Wer diese Standards verwendet, muss Maßnahmen zur Bewertung der CMS vorweisen können.

» In welchen Abständen sollten Unternehmen ihre Compliance-Daten auswerten, um aussagekräftige Ergebnisse zu erhalten?

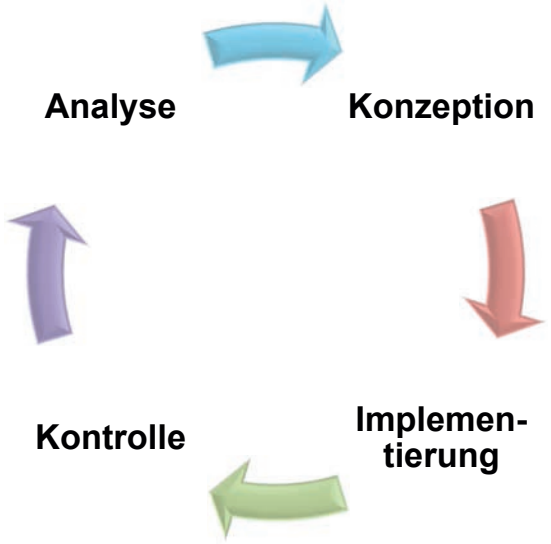
« Die Auswertung und Analyse der Compliance-Daten insgesamt sollte natürlich kontinuierlich erfolgen. Es ist gängige Praxis, operative Daten mindestens monatlich zu berichten. Hierzu gehören zum Beispiel der Status durchgeführter Schulungen, die Auswertung des Zuwendungsregisters, oder auch Ergebnisse sogenannter 3rd-Party-Due-Diligence. Darüber hinaus gibt es Compliance-Aktivitäten, die eher jährlich vorgenommen werden. Hierzu zählen die grundsätzliche Review des Risikokatalogs oder auch Mitarbeiterbefragungen mit den entsprechenden Reports. Insgesamt gilt natürlich auch, dass die Tiefe und Frequenz der Datenerhebung und des zugehörigen Berichtens in erster Linie von der Situation der Organisation abhängig sind und somit dem Prinzip der Angemessenheit unterliegen. *chk*


Michael Kayser

Michael Kayser, Geschäftsführer Idox Compliance, war aktives Mitglied im Arbeitskomitee zur Entwicklung der ISO 37001. Er war zuvor bereits als einer der deutschen Vertreter aktiv an der Entstehung der ISO 19600 beteiligt.

In vier Schritten zur Corporate Compliance

Die Notwendigkeit, ein Compliance-System einzuführen, liegt für viele Geschäftsleiter inzwischen auf der Hand. Doch wie gelingt die organisatorische Umsetzung im Unternehmen? Nikolai Unmuth erkärt, wie ein auf den Einzelfall abgestimmtes Compliance-System in vier Schritten aufgebaut werden kann.



Kreislauf in vier Schritten: Das Compliance-System muss fortlaufend auf Effizienz und Geeignetheit überprüft werden.

Einige Gesetze enthalten genaue Vorgaben dazu, welche Compliance-Maßnahmen von bestimmten Unternehmen ergriffen werden müssen. „Insbesondere Kredit- und Finanzdienstleistungsunternehmen, Wertpapierdienstleistungsunternehmen, Kapitalverwaltungsgesellschaften, Zahlungsinstitute und Versicherungsunternehmen sind von spezialgesetzlichen Compliance-Vorgaben betroffen. Wer keiner spezialgesetzlichen Compliance-Pflicht unterfällt, ist im Umkehrschluss jedoch nicht von jeglicher Compliance-Pflicht frei", stellt Nikolai Unmuth klar und empfiehlt die Umsetzung der Corporate Compliance in vier Schritten: Analyse, Konzeption, Implementierung und Kontrolle.

„Bei der Analyse geht es darum, herauszufinden, bezüglich welcher Rechtsverstöße aufgrund der Branche oder der Erfahrungen aus der Vergangenheit ein erhöhtes Risikopotential besteht", so Unmuth. Außerdem sei zu ermitteln, ob die vorhandene Unternehmensstruktur und Unternehmenskultur Rechtsverstöße eher begünstigen oder erschweren.

Ziel der Compliance-Konzeption müsse es sein, die in der Analyse festgestellten Risiken abzudecken. Dazu gehört laut Unmuth auch, die Effektivität der in der Vergangenheit getroffenen Compliance-Maßnahmen zu berücksichtigen. Bei der Suche nach geeigneten, bisher noch nicht ergriffenen Maßnahmen solle auf wissenschaftlich anerkannte oder praxisgeprüfte Compliance-Elemente zurückgegriffen werden. „Hierzu können Gerichtsentscheidungen und juristische Fachbeiträge, aber auch die einschlägigen OECD-Richtlinien, der IDW-PS 980, die Organizational Sentencing Guidelines aus den USA oder spezialgesetzliche Vorgaben, wie z. B. in §§ 33 WpHG, 12 WpDVerOV verwendet werden." Am Ende aber hänge vom Einzelfall ab, was geboten sei: „Eine pauschale Checkliste gibt es nicht", macht Unmuth deutlich.

Zur Implementierung empfiehlt Unmuth, dass sich das Unternehmen öffentlich zu Compliance bekennt – zum Beispiel in einem Mission Statement. Entscheidend sei aber die Integration von Compliance in die Unternehmenskultur: „Letztlich muss das gesamte Unternehmen Compliance in einer Art Lernprozess aufnehmen und verinnerlichen."

Der vierte Schritt der Kontrolle baue eine Brücke zurück zum ersten Schritt, der Analyse: „Werden im Rahmen der Kontrolle (Schritt 4) Unstimmigkeiten entdeckt, sind diese sofort zu analysieren (Schritt 1), geeignete Gegenmaßnahmen zu konzipieren (Schritt 2) und umzusetzen (Schritt 3)," beschreibt Unmuth den Kreislauf des Compliance-Systems, das fortlaufend auf seine Effizienz und Geeignetheit zu überprüfen sei. *chk*

Auf einen Blick:

Gesellschaften, die keiner spezialgesetzlichen Compliance-Pflicht unterliegen, müssen in eigener Verantwortung die für sie passenden Compliance-Elemente in ihren Unternehmen umsetzen. Dazu empfehlen sich vier Schritte:

- Analyse der Risiken
- Konzeption zur Abdeckung der Risiken
- Implementierung des Compliance-Systems
- Kontrolle der Effizienz und Geeignetheit

Nikolai Unmuth, LL.M. (USC), Dipl.-Jur. Univ., ist seit 2015 Wissenschaftlicher Mitarbeiter im Stuttgarter Büro der Rechtsanwaltskanzlei Gleiss Lutz. Im Rahmen dieser Tätigkeit ist er häufig mit Compliance-Themen befasst. Er promoviert außerdem an der Universität Tübingen zu einem Thema aus dem aktienrechtlichen Organhaftungsrecht.

Als Leser von „Compliance" erhalten Sie **hier** exklusiv den Zugang zum ausführlichen Beitrag „Die organisatorische Umsetzung der Corporate Compliance" von Nikolai Unmuth im Compliance Berater, Ausgabe Juni 2017.

News

Weitere Millionen-Bußgelder fallen durch „Wurstlücke"

Wie das Bundeskartellamt Ende Juni mitteilte, muss es weitere Bußgeldverfahren in Millionenhöhe einstellen. Der Grund hierfür ist eine bis Anfang Juni geltende gesetzliche Regelungslücke im Kartellrecht, die seit einem Verfahren gegen Wursthersteller im Jahr 2014 als „Wurstlücke" bekannt ist. Jüngst hat das Bundeskartellamt Bußgeldbescheide gegen die Bell Deutschland Holding GmbH in Höhe von 99,6 Mio. Euro, gegen die Marten Vertriebs GmbH & Co. KG in Höhe von 3,2 Mio. Euro und gegen die Sickendiek Fleischwarenfabrik GmbH & Co. KG in Höhe von 6,9 Mio. Euro aufgehoben. Andreas Mundt, Präsident des Bundeskartellamtes, erkärt hierzu: „Die Einstellung der Verfahren ließ sich aufgrund der bis vor Kurzem noch geltenden gesetzlichen Lage nicht verhindern. Allein in diesem Verfahren sind damit Bußgelder in einer Gesamthöhe von rund 238 Mio. Euro entfallen. Mit der aktuellen Novelle des Gesetzes gegen Wettbewerbsbeschränkungen wurde dieses Schlupfloch jedenfalls für neue Verfahren geschlossen. Es gilt nun – wie auf europäischer Ebene – eine Unternehmensverantwortlichkeit. Damit müssen nun auch lenkende Konzernmütter für die Bußgelder mit einstehen."

Zuvor hatte das Bundeskartellamt bereits das Bußgeldverfahren gegen zwei Gesellschaften der Zur Mühlen-Gruppe einstellen müssen. Die gegen die Böklunder Plumrose GmbH & Co. KG, Böklund, sowie die Könecke Fleischwarenfabrik GmbH & Co. KG, Bremen, erlassenen Bußgeldbescheide über insgesamt 128 Mio. Euro waren damals ebenfalls infolge konzerninterner Umstrukturierungen gegenstandslos geworden.

Compliance-konformes Personalmanagement

Die Personalabteilung muss wie jede andere Abteilung auch die eigenen Prozesse im Sinne von Compliance führen und „pflegen", d. h. überwachen. Hierzu sind Mitarbeiter nicht nur im Rahmen von Audits zu prüfen, sondern vor allem primär darüber aufzuklären, was Compliance im Unternehmen bedeutet und was dies für den Arbeitsalltag konkret heißt.

Rawpixel/iStock/Thinkstock

Präsenzschulung: Compliance – insbesondere mit und durch HR – kann nur funktionieren, wenn sachgerecht aufgeklärt und der sog. „tone from the top" wahrgenommen wird.

Mögliche Inhalte einer Compliance-Richtlinie für den Personalbereich

A. Einleitung: Erläuterungen zu Compliance (im Allgemeinen)
   Ausgangssituation – Zielsetzung - Anwendungsbereich
B. Arbeitsrechtliche Umsetzung von Compliance-Regelungen
C. Arbeitsrechtliche Rahmenbedingungen bei der Ermittlung und Aufdeckung von Compliance-Verstößen
   Erläuterungen des Sanktionen-Systems: Grundsätze – Maßnahmen – Durchführung – Arbeitsrechtliche Folgen
D. Arbeitsrechtlich relevante Gesetze und sonstige Standards (ggf. auch Bezug und Verhältnis zu implementierten ISO/DIN-Standards)
   Grundsätze – AGG – Arbeitszeitgesetz – Arbeitsschutzgesetz – AÜG – BetrVG – Datenschutz etc.
E. Folgen bei Verstößen
F. Meldung von Verstößen/Verdachtsfällen: Aufklärungsprinzip – Verfahren – Abläufe
G. Schulungsmaßnahmen/Weiterbildung
H. Bekanntmachung
I. Beteiligung des BR
J. Ansprechpartner bei Fragen
   Aktuelle Kontaktdaten der Compliance-Abteilung vor Ort und der „zentralen Compliance-Einheit" sowie alternativ Kontaktpersonen aus dem Bereich Personal und möglicherweise der Spezialausschuss des BR zu Compliance/Revision.

Arbeitnehmer zu überprüfen ist für Compliance ein Mittel zum Zweck, jedoch muss es bereits im Vorfeld zu entsprechenden Maßnahmen kommen. Die Arbeitnehmerschaft sowie das Management müssen die hauseigenen Spielregeln und Gesetze letztlich kennen und einhalten. Damit dies gewährleistet ist, müssen in jedem Fall Schulungsmaßnahmen ergriffen werden. Eine flexible Handhabung bieten hier insbesondere die klassischen Online-Schulungstools. Es geht jedoch vielmehr darum, auch durch Präsenzschulungen den Mitarbeitern Rede und Antwort zu stehen, so dass eine wirkliche Aufklärung stattfinden kann und die Anwendung auf die Prozesse im „täglichen doing" erfolgt.

Eine Kombination aus Online- und Präsenzschulungen ist mit Sicherheit effektiver als eine bloße Aufklärung aus der Ferne. Dies führt im Ergebnis zu dem Punkt, dass Compliance – insbesondere mit und durch HR – nur funktionieren kann, wenn sachgerecht aufgeklärt und der sog. „tone from the top" wahrgenommen wird. Nur so verstehen Mitarbeiter Compliance und können im Unternehmen einen Beitrag dazu leisten, dass die Compliance-Kultur hierzu weitergetragen wird.

Hierbei geht es auch darum, den Fachbereichen aufzuzeigen, wo die jeweiligen Kernprobleme liegen können, und, dass diese Informationen organisatorisch bereitzustellen oder zumindest abrufbar zu machen sind. Dies kann bei Einstellung durch eine Mitarbeitermappe geschehen und im Rahmen des Arbeitsverhältnisses durch entsprechende Mediatheken, welche für jeden Mitarbeiter aktuelle Informationen und Hinweise bereit halten. Selbstverständlich ist auch an dieser Stelle dafür zu sorgen, dass Informationen bereit stehen und dass Compliance in die Kommunikation einzubinden ist.

Die Personalabteilung erfüllt durch die Wahrnehmung dieser Maßnahmen selbst wiederum die Anforderung, compliance-konform zu managen und zu kommunizieren. Dies sollte im Zweifel ohnehin in der unternehmenseigenen HR-Richtlinie geregelt sein.

Der Sinn und Zweck von Richtlinien ist vor allem die Dokumentation und Transparenz wesentlicher Regelungen sowie das Aufzeigen von Konsequenzen bei Missbrauch oder Nichtbefolgen. Damit bringt das Unternehmen letztlich auch den Nachweis darüber, dass Compliance gelebt wird und wirkt somit auf seine Verpflichtung hin, auch tatsächlich der „ehrbare Kaufmann" zu sein. Zusätzlich kann dokumentiert werden, dass ein CMS besteht und Neuerungen sowie Anpassungen der Inhalte so im Zusammenhang kommuniziert werden. Im Ergebnis besteht eine einheitliche Kommunikationsbasis, welche bei den jeweiligen Fragestellungen oder Bedenken zur Anwendung kommt.

HR-Compliance bedeutet im Ergebnis nicht nur regelkonformes Verhalten der Mitarbeiter, sondern eben auch ein regeltreues Verhalten der Personalabteilung, welche die Möglichkeit hat, den sog. „tone from the top" in die entsprechenden Mitarbeiterebenen zu kommunizieren und gezielt darauf hinzuwirken, dass Compliance gelebt wird. Dabei ist der Personalbereich auch Sprachrohr für das Management und die Unternehmenswerte auf allen Ebenen; und dies neben den eigenen Anforderungen, welche dieser Bereich ohnehin pflegen muss, wie u. a. das korrekte Verwalten von personenbezogenen Daten, Gleichbehandlungsrechte, Schwerbehindertenrechte oder das Einhalten der sonstigen arbeitsrechtlichen Vorschriften sowohl in der Bewerbungsphase als auch im Rahmen der Kündigung.

Jasmin und Armin Fladung, CAD-Institut

EU-Datenschutzgrundverordnung: Auswirkungen auf die Compliance

Am 25. Mai 2018 wird die zweijährige Übergangsfrist der Datenschutzgrundverordnung (DSGVO) ablaufen; ab diesem Datum wird die DSGVO verbindlich angewendet. In unserem fünften Beitrag in der Reihe „Compliance-Praxis in der DACH-Region" erläutern Dr. Michael Widmer und Stefan Hegyi am Beispiel Schweiz, warum die DSGVO auch Unternehmen außerhalb der EU betrifft.

Augen auf beim Datenschutz: Auch Unternehmen außerhalb der EU können den Regeln der DSGVO unterliegen.

Die DSGVO regelt in der EU die Verarbeitung von personenbezogenen Daten natürlicher Personen, einschließlich deren Erhebung, Verwendung und Löschung. Sie ist zwar bereits am 24. Mai 2016 in Kraft getreten, wird aber erst nach Ablauf einer Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam. Auf dieses Datum müssen sich Unternehmen indessen vorbereiten und bis dahin die Umsetzung der DSGVO sicherstellen.

Betroffen davon sind nicht nur Unternehmen mit Sitz in der EU. Die DSGVO ist anwendbar, wenn die Verarbeitung im Rahmen der Tätigkeiten einer EU-Niederlassung, eines Verantwortlichen oder eines Auftragsbearbeiters erfolgt (Art. 3 Abs. 1 DSGVO). Die Anwendbarkeit ist indessen nicht davon abhängig, ob die Verarbeitung selbst in der EU stattfindet. Demnach kann die DSGVO auch auf Schweizer Unternehmen (oder andere Firmen außerhalb der EU) anwendbar sein, (a) die Personendaten durch einen Auftragsdatenbearbeiter in der EU verarbeiten lassen (z. B. Cloud-Anbieter), (b) auf die Datenverarbeitung der EU-Niederlassung eines schweizerischen Unternehmens oder (c) auf die Verarbeitung von Personendaten durch ein Schweizer Unternehmen als Auftragsbearbeiter eines EU-Unternehmens. Damit aber nicht genug: Die DSGVO führt darüber hinaus das so genannte „Marktortprinzip" ein. So gilt die DSGVO auch für Datenverarbeitungen durch Verantwortliche oder Auftragsbearbeiter ohne Niederlassung in der EU, wenn Daten von Personen verarbeitet werden, die sich in der EU befinden, und (a) die Datenverarbeitung mit einem Angebot von Waren oder Dienstleistungen an betroffene Personen in der EU im Zusammenhang steht; oder (b) die Verarbeitung im Zusammenhang steht mit einer Beobachtung des Verhaltens von Personen, soweit das Verhalten in der EU erfolgt. Die DSGVO wird demnach nicht nur von deutschen und österreichischen Unternehmen, sondern auch von einer großen Zahl von Schweizer Unternehmen zu beachten sein.

In der Schweiz soll ferner das Bundesgesetz über den Datenschutz („DSG") revidiert werden. Der Schweizer Bundesrat hat kurz vor Weihnachten 2016 den ersten Entwurf hierzu in die Vernehmlassung geschickt. Das revidierte DSG wird der DSGVO zumindest ähnlich sein und soll einen angemessenen Schutz im Sinne der DSGVO garantieren. Es ist deshalb zu erwarten, dass sich Schweizer Unternehmen bei der Umsetzung der revidierten Datenschutzregelungen an der deutschen und österreichischen Compliance-Praxis zumindest orientieren können, selbst wenn die DSGVO nicht auf sie anwendbar sein sollte.

Die DSGVO sieht einen erheblich erhöhten Bußgeldrahmen vor. Je nachdem, gegen welche Bestimmung verstoßen wird, können Geldbußen von bis zu € 20 Mio. oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden. Auch im Entwurf für ein revidiertes Schweizer DSG sind Bußen bis zu CHF 500.000 vorgesehen. Diese Umstände führen unter anderem dazu, dass der Datenschutz in Unternehmen immer mehr zu einem Thema wird. Der Umsetzung der DSGVO sowie allenfalls des künftig revidierten DSG sollte dementsprechend gerade in der Compliance ein hoher Stellenwert beigemessen werden.

Ferner sieht die DSGVO diverse Neuerungen vor, unter anderem

- erweiterte Dokumentations- und Nachweispflichten (bspw. Art. 5 Abs. 2 sowie Art. 24 Abs. 1 DSGVO)
- erweiterte Transparenzvorschriften (bspw. Art. 5 Abs. 1 sowie Art. 12 bis 15 DSGVO)
- Vorgaben für Datenschutz durch Technik (Privacy by Design; Art. 25 Abs. 1 DSGVO) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default; Art. 25 Abs. 2 DSGVO)
- Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen (Art. 33 und 34 DSGVO)
- Datenschutz-Folgenabschätzung
- Löschen von Daten und Recht auf Vergessenwerden (Art. 17 DSGVO)

Als Basis für Compliance-Maßnahmen im Datenschutzbereich muss zunächst der „Ist-Zustand" festgestellt werden. Erst gestützt darauf (sowie den „Soll-Zustand") kann gegebenenfalls eine rechtliche Beurteilung stattfinden, ob Abweichungen bestehen, eine Risikoanalyse durchgeführt und „To Dos" herausgearbeitet werden, welche es sodann umzusetzen gilt. Erfahrungsgemäß nimmt die Feststellung des „Ist-Zustandes", insbesondere der relevanten Datenverarbeitungen und Datenflüsse mehr Zeit in Anspruch, als dies oftmals angenommen wird.

Dr. Michael Widmer und Stefan Hegyi

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

Dr. Michael Widmer, LL.M., ist als Rechtsanwalt in Zürich tätig. Zudem ist er Dozent an der ZHAW School of Management and Law sowie am Zürcher Zentrum für Informationstechnologie und Datenschutz (ITPZ), einem Verein zur Förderung, Umsetzung und Weiterentwicklung des Datenschutzes, den die ZHAW zusammen mit dem Datenschutzbeauftragten des Kantons Zürich gegründet hat.

Stefan Hegyi, MLaw, ist wissenschaftlicher Mitarbeiter an der ZHAW School of Management and Law sowie am Zürcher Zentrum für Informationstechnologie und Datenschutz (ITPZ). Er berät zu technisch geprägten Rechtsfragen, insbesondere Datenschutz.