Was man hat, das hat man

Nachricht vom 30.09.2015

Die Mehrheit der IT-Entscheider in deutschen Unternehmen wünscht sich eine Lockerung der Zweckbindung von personenbezogenen Daten, so das Ergebnis der Studie „Digital Security" von Sopra Steria.

Daten sind das Öl unserer Zeit. Kein andere „Rohstoff" verspricht mehr Fortschritt und Innovation als die unzähligen digitalen Fußspuren, die wir als Nutzer hinterlassen, sei es wenn wir im Internet einkaufen, Videos schauen oder uns via Navigations-App zu unserem Lieblingscafé leiten lassen. Aber auch eine Autofahrt produziert Unmengen an wertvollen Daten, die für die Industrie interessant sind.

Das Sammeln personenbezogener Daten ist aber nicht ohne weiteres möglich. Der Grund: Die auf die Volkszählung 1983 zurückgehende Regelung zur Zweckbindung sieht vor, dass personenbezogene Daten nur dann erhoben werden dürfen, wenn die Verwendung vorab festgelegt ist. Mit dem sogenannten Volkszählungsurteil wurde erstmals das Grundrecht auf informationelle Selbstbestimmung als grundlegendes Persönlichkeitsrecht festgeschrieben – und ist seitdem ein Eckpfeiler des Datenschutzes.

Datenschutz spaltet die IT-Experten

Diese Restriktion wollen die Mehrheit der IT-Entscheider in den Unternehmen – so die Studie „Digital Security" der Unternehmensberatung Sopra Steria Consulting – gerne lockern. Ihr Argument: Die gewinnbringende Art der Nutzung von Informationen ergebe sich oftmals erst, nachdem die Daten erhoben wurden. Daher plädieren sie dafür, mehr Daten auf Vorrat zu sammeln, ganz nach dem Motto: „Was man hat, das hat man".

Ein Drittel der Befragten wäre im Gegenzug bereit, mehr in Prozesse und Softwareprogramme zu investieren, um Daten besser auswerten zu können bei gleichzeitiger Einhaltung der IT-Sicherheits- und Datenschutzanforderungen. 16 Prozent hingegen sehen selbst hierfür keine Notwendigkeit und treten nur für eine Lockerung ein. Auf der anderen Seite sprechen sich fast 50 Prozent für die Beibehaltung der Zweckbindung aus, auch wenn das bedeutet, dass bestimmte Auswertungen nicht gemacht werden können.

Für Gerald Spiegel, Leiter Information Security Solutions bei Sopra Steria, bedeutet eine Lockerung der Zweckbindung nicht automatisch eine Abschaffung des Datenschutzes: „Unternehmen könnten zum Beispiel ein Mindestmaß an Sicherheit gewährleisten, wenn sie garantieren, dass Daten nicht an Dritte weitergegeben werden und dass jegliche Änderungen in der Datennutzung dokumentiert werden", so Spiegel.

Verarbeitendes Gewerbe will von Nutzerdaten profitieren

Laut der Umfrage treten vor allem IT-Entscheider aus dem verarbeitenden Gewerbe für eine Lockerung ein. Hier wollen mehr als zwei Drittel die bestehenden Regelungen ändern. Dagegen wollen auf der anderen Seite zwei Drittel der IT-Entscheider aus der Finanzbranche an den aktuellen Regeln festhalten.

Auffällig an dem Ergebnis ist, dass es bei der Digitalisierung der Industrie vor allem um die Auswertung von Maschinen- und nicht von Nutzerdaten geht. Aus Sicht von Lars Schlömer, Leiter Business Intelligence bei Sopra Steria, zeigt dies, dass vor allem Unternehmen aus dem verarbeitenden Gewerbe auf der Suche nach neuen Geschäftsmodellen jenseits des Kerngeschäftes sind. So können z. B. Automobilzulieferer dank der Echtzeitüberwachung der Fahrzeugtechnik rechtzeitig vor Materialverschleiß warnen oder – so eine andere denkbare Anwendung – Hinweise zur Reduzierung des Spritverbrauchs geben. Hierdurch erhalten sie die Möglichkeit, so Schlömer, „die Wertschöpfung, die bislang mit dem Verkauf der Technik an einen Automobilzulieferer endete, zu erweitern".

Geschäft trotz Datenschutz

Einen anderen Weg schlägt der US-amerikanische Konzern Apple ein. Erst gestern wurde eine neue Seite des Unternehmens zum Thema Datenschutz ins Netz gestellt: Darin bewirbt Apple die Datenschutzbestimmungen des Unternehmens. Der Grundtenor: „Die persönlichste Technologie muss absolut privat bleiben". Ob die Strategie von Apple – Datenschutz als Verkaufsargument zu positionieren – aufgeht, bleibt abzuwarten. Letztlich entscheiden auch die Kunden, ob und was ihnen der Schutz der eigenen Daten wert ist. (ESV/ms mit Material von Sopra Steria Consulting)

Literaturhinweise zum Thema Datenschutz

Über aktuelle und grundlegende Fragen zum Datenschutz, informiert die Zeitschrift PinG – Privacy in Germany (http://www.compliancedigital.de/short/ping/ejournal-inhalt.html). Abonnenten von COMPLIANCEdigital lesen PinG kostenfrei!

IT-Sicherheitsgesetz: Zeit für eine erste Bilanz

Nachricht vom 24.09.2015

Seit 100 Tagen ist das IT-Sicherheitsgesetz nun in Kraft. Wie bewerten IT-Experten das neue Gesetz? Eine Studie von Sopra Steria zeichnet ein sehr durchwachsenes Bild.

Lange wurde um das IT-Sicherheitsgesetz gerungen – auch unter Beteiligung der deutschen Industrie (http://www.compliancedigital.de/ce/neue-gesetzesvorlage-fuer-mehr-it-sicherheit-in-deutschland/detail.html). Im Juni dieses Jahres trat das Gesetz in Kraft. Nach guter parlamentarischer Tradition ist nach 100 Tagen die Schonfrist vorbei – und Zeit für eine erste Zwischenbilanz: Wie bewerten die IT-Entscheider in den Unternehmen das neue Gesetz? Um die Frage zu beantworten, hat die Management- und Technologieberatung Sopra Steria 110 IT-Entscheider aus Unternehmen ab 500 Mitarbeitern befragt. Die Ergebnisse sind in die Studie „Digital Security" eingeflossen.

IT-Sicherheitsgesetz spaltet die Branche

Die Meinungen zum IT-Sicherheitsgesetz gehen in der Branche weit auseinander. Zwar begrüße die Mehrheit der Befragten das neue Gesetz als einen Schritt in die richtige Richtung. Jeder fünfte jedoch hält das Gesetz in dieser Form für unzureichend und fordert eine strengere Regulierung, wohingegen 13 Prozent der Befragten die neuen Regelungen für zu streng halten.

Das IT-Sicherheitsgesetz verpflichtet Betreiber sogenannter „kritischer Infrastrukturen" ein Mindestniveau an IT-Sicherheit einzuhalten. Zudem müssen sie IT-Sicherheitsvorfälle dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Hard- und Software-Hersteller sind ebenfalls zur Mitwirkung bei der Beseitigung von Sicherheitslücken verpflichtet.

IT-Sicherheitsgesetz muss zunächst durchgesetzt werden

Aus Sicht von Sopra Steria ist es allerdings noch zu früh, Veränderungen – ganz gleich ob Verschärfungen oder Aufweichungen – an dem Gesetz zu fordern. Nach Auffassung von Gerald Spiegel, Leiter Information Security Solutions bei Sopra Steria, müsse das Gesetz zunächst einmal in seiner heutigen Form durchgesetzt werden. Klar sei aber auch, dass Betreiber kritischer IT-Infrastrukturen, die den Vorgaben des Gesetzes nicht nachkommen, „entsprechend sanktioniert werden" müssen.

Sanktionshöhe ist zu gering

Zu hinterfragen ist aber nach Ansicht von Spiegel bereits heute die Höhe möglicher Sanktionszahlungen. Laut des energiewirtschaftlichen Instituts an der Universität Köln verursache ein einstündiger Stromausfall durchschnittliche Wertschöpfungsverluste von 430 Millionen Euro. Wenn der Stromausfall aber durch eine unzureichende IT-Sicherheit ausgelöst wurde, steht ein Bußgeld von maximal 100.000 Euro dazu in keiner Relation", so Spiegel. (ESV/ms mit Material von Sopra Steria)

Literaturhinweise zum Thema IT-Sicherheit

Wie Unternehmen wesentliche regulatorische Anforderungen an die IT identifizieren, priorisieren und deren Erfüllung einer effizienten Steuerung zuführen, erläutern Michael Rath und Rainer Sponholz in dem Band „IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen (http://www.compliancedigital.de/ce/it-compliance-7/ebook.html)".

Eine praxisorientierte Einführung in die Welt der IT-Prüfung bietet Stefan Beißel in „IT-Audit: Grundlagen – Prüfungsprozess – Best Practice (http://www.compliancedigital.de/ce/it-audit/ebook.html)". Anhand eines umfassenden Prüfungskatalogs können Sie systematisch erschließen, worauf es bei der Vorbereitung, der Durchführung und dem Abschluss erfolgreicher IT-Audits ankommt.

Volkswagen USA: Wo war die Compliance?

Nachricht vom 22.09.2015

Der Abgas-Skandal von Volkswagen in den USA offenbart gravierende Compliance-Lücken. Beobachter fragen sich, ob VW aus den Fehlern der Vergangenheit nichts gelernt habe?

Der Volkswagen Konzern – und damit auch die deutsche Wirtschaft – wird von einem veritablen Manipulations-Skandal erschüttert. Gerade wurden auf der weltgrößten Automobilausstellung in Frankfurt (IAA) die neuesten Modelle präsentiert, da platzte die Bombe. Der Vorwurf: der Konzern – wie inzwischen auch offiziell bestätigt – soll eine spezielle Software entwickelt und eingesetzt haben, um die Messung des Schadstoffausstoßes in seinen Diesel-Fahrzeugen zu manipulieren, so die US-Umweltbehörde EPA. Das gesamte Ausmaß dieses Skandals ist noch gar nicht absehbar. Im schlimmsten Fall droht dem VW-Konzern, der sich anschickte nicht nur der weltweit größte Automobilbauer sondern auch der Technologieführer in der Branche zu werden, eine Milliardenstrafe von 18 Milliarden Dollar. Hinzu kommt ein Imageschaden, der nicht nur VW, sondern die gesamte deutsche Automobilindustrie treffen könne.

Um die Dimension zu verstehen, was dem VW-Konzern droht, reicht ein Blick in die Bilanzen: Der Konzerngewinn im Jahr 2014 lag bei 12,7 Milliarden Euro (rund 14 Milliarden Dollar). Der Amerika-Chef von Volkswagen, Michael Horn, hat bei der Präsentation des neuen Passat in New York in seltener Offenheit zwar schon zugegeben, dass VW es „verbockt" hat und gleichzeitig auch angekündigt, „bezahlen, was wir zu bezahlen haben". Am Ende, so viel ist sicher, wird dies aber nicht reichen. Längst wird auch über personelle Konsequenzen – mehr oder weniger laut – nachgedacht. Laut Informationen des Tagesspiegels soll der VW-Chef Martin Winterkorn noch diese Woche abgelöst werden.

Zuvor müssen aber einige Fragen geklärt werden: Wie konnte das passieren? Wer wusste davon? Wer hat die Manipulation angeordnet? Und haben die Verantwortlichen wirklich geglaubt, dass der Betrug nicht auffliegt?

Hat die Compliance versagt?

Der Automobilexperte Prof. Dr. Stefan Bratzel von der Fachhochschule der Wirtschaft in Bergisch Gladbach legt den Finger noch tiefer in die Wunde, wenn er Handelsblatt die Frage stellt, wo denn die Compliance gewesen sei? Leicht verwundert fragt sich Bratzel, ob man sich in Wolfsburg nicht im Klaren gewesen ist, „dass man Regeln nicht einfach aushebeln darf".

US-Justizbehörde ermittelt

Antworten – nicht nur auf diese Fragen – wird der Konzern in naher Zukunft beantworten müssen. Die US-Justizbehörde hat bereits angekündigt, gegen VW zu ermitteln, wie das Handelsblatt unter Berufung auf Quellen der Nachrichtenagentur Bloomberg berichtet. Und auch für die Verantwortlichen selbst kann es ungemütlich werden. Wie das US-Justizministerium in September in einem Memorandum angekündigt hat, werde man sich in Zukunft verstärkt auf das Fehlverhalten der einzelnen Verantwortlichen konzentrieren: „Eine der mächtigsten Waffen gegen Fehlverhalten ist es, die Verantwortlichen direkt zur Rechenschaft zu ziehen." Mit diesem Vorgehen, so die Begründung der Justizbehörde „verringere man die Wahrscheinlichkeit eines erneuten Fehlverhaltens" und „stelle sicher, dass die Richtigen getroffen" würden.

Compliance bei VW: Alles unter Kontrolle – dachte man

Noch im Juni sah sich Volkswagen in Sachen Compliance auf einem guten Weg. Zehn Jahre nach dem großen Skandal von Schmiergeldzahlungen und Lustreisen auf Firmenkosten versicherte der Chief Compliance Officer von Volkswagen, Dr. Frank Fabian, gegenüber der Deutschen Presseagentur, dass man Regelverstöße möglichst schon im Vorfeld ausschließen wolle und deshalb stark auf Prävention setze. Auch der Leiter der Konzernrevision Peter Dörfler sagte, dass grundsätzlich alle Abläufe im Unternehmen geprüft werden. „Darüber hinaus nehmen wir verdachtsunabhängige Kontrollen und im Verdachtsfall intensive Untersuchungen vor", so Dörfler. Anscheinend wurden einige wichtige Abläufe in den USA vergessen. Man darf gespannt sein, was im Laufe der Ermittlungen noch alles zu Tage getragen wird. Die Erfahrung zeigt, dass Compliance-Verfehlungen – leider – keine Einzelhandlung, sondern oftmals einen systemischen Hintergrund haben.

Literaturempfehlung zu Compliance

In dem Handbuch Compliance international (http://www.compliancedigital.de/ce/handbuch-compliance-international/ebook.html) geben Experten einen umfassenden Überblick über die Grundlagen compliance-relevanter Rechtsgebiete bedeutender Wirtschaftsnationen – auch der USA Über die Führungsaufgaben und Rechtspflichten eines Vorstandes einer Aktiengesellschaft informiert

der Band Vorstand der AG (http://www.compliancedigital.de/ce/vorstand-der-ag-1/ebook.html), herausgegeben von Dr. Jürgen van Kann. Der Band hilft Ihnen, die wesentlichen Haftungsfallen zu erkennen und zu vermeiden. Behandelt werden auch Themen wie Vergütungsfragen, D&O-Versicherung und Compliance.

Der Umgang mit informellen Gruppen

Nachricht vom 08.09.2015

Informelle Gruppen stellen die Compliance vor vielfältige Herausforderungen. Wie gegen informelle Gruppen vorgegangen werden kann, beschreibt Thomas Schneider im 6. Teil der Serie Mitarbeiter-Compliance.

Wenn die Compliance Gruppen identifiziert hat, die eine hohe Risikoausprägung (siehe hierzu den 6. Teil der Serie Mitarbeiter-Compliance (http://www.compliancedigital.de/ce/informelle-gruppen-herausforderung-fuer-die-compliance/detail.html)) aufweisen, muss aus Sicht der Compliance schnell gehandelt werden.

Schwächung des Gruppenzusammenhalts

Bei zu starken Gruppenzusammenhalt gibt es nur ein adäquates Gegenmittel: Veränderungen. Hierzu muss der Zusammenhang der Gruppe geschwächt werden, indem z. B. neue Mitglieder in die Teams integriert werden.
Ergänzende Maßnahmen sind:

- Räumliche Trennung der Mitglieder
- Erhöhung der Gruppengröße
- Reduzierung der Gruppenzusammenkünfte
- Erhöhung des Konkurrenzdenkens, Aufteilung in Untergruppen und Vergleich des Ergebnisses

Veränderung der Gruppendynamik

Ein wichtiger Schritt ist die Änderung der Gruppendynamik. Gruppen in schrumpfenden Tätigkeitsfeldern werden hierzu neue Mitglieder zugeführt. Dazu ist eine Attraktivitätssteigerung erforderlich, etwa beim Gehalt und den Entwicklungsmöglichkeiten. Loyale und erfahrene Kräfte werden wiederum in Gruppen in Wachstumsbereichen zugeordnet.

Auswege aufzeigen

In der Phase der Desorientierung suchen Mitläufer zudem nach Auswegen. Wenn im Unternehmen bereits entsprechende Möglichkeiten bestehen, bspw. ein Ombudsmann zur Verfügung steht, sollten diese Ansprechpartner nochmals vorgestellt werden. Anderenfalls sind entsprechende Möglichkeiten zur schaffen.

Serie Mitarbeiter-Compliance

- Teil 1: Compliance: Ein Thema aller Mitarbeiter (http://www.compliancedigital.de/ce/compliance-ein-thema-aller-mitarbeiter/detail.html)
- Teil 2: Was Compliance-Verantwortliche von Geheimdiensten lernen können (http://www.compliancedigital.de/ce/was-compliance-verantwortliche-von-geheimdiensten-lernen-koennen/detail.html)
- Teil 3: Die Welt vor Compliance (http://www.compliancedigital.de/ce/die-welt-vor-compliance/detail.html)
- Teil 4: Einstieg ins Unternehmen (http://www.compliancedigital.de/ce/einstieg-ins-unternehmen-1/detail.html)
- Teil 5: Ausscheidende Mitarbeiter (http://www.compliancedigital.de/ce/ausscheidende-mitarbeiter/detail.html)
- Teil 6: Informelle Gruppen: Herausforderung für die Compliance (http://www.compliancedigital.de/ce/informelle-gruppen-herausforderung-fuer-die-compliance/detail.html)
- Teil 7: Der Umgang mit informellen Gruppen

Zur Person

Dipl.-Kaufmann Thomas Schneider ist für die Corporate Compliance der Knauf Interfer SE verantwortlich, einem führenden Distributions-, Service- und Bearbeitungsunternehmen für Stahl und Aluminium. Er ist Verfasser zahlreicher Veröffentlichungen zur Compliance. Im Erich Schmidt Verlag ist der Band Mitarbeiter-Compliance erschienen.

Literaturhinweis

Weitere Informationen zu dem Thema gibt das Buch „Mitarbeiter Compliance (http://www.compliancedigital.de/ce/mitarbeiter-compliance/ebook.html)". Das eBook steht Abonnenten von COMPLIANCEdigital ebenfalls kostenfrei zur Verfügung.

Informelle Gruppen: Herausforderung für die Compliance

Nachricht vom 04.09.2015

Organigramme helfen der Compliance, die Struktur eines Unternehmens zu überblicken. Aber zeigen sie wirklich alles? Nein, sagt Thomas Schneider. Insbesondere informelle Gruppen stellen die Compliance vor große Herausforderungen.

Eine Grundvoraussetzung für die Compliance ist es, die Struktur eines Unternehmens vollständig zu erfassen: Wer berichtet an wen und wo bestehen möglicherweise Abhängigkeiten oder Funktionsüberschneidungen? Organigramme und Funktionsbeschreibungen geben einen ersten Überblick. Aber: Sie zeigen nur die „offizielle" Seite!

Informelle Abhängigkeiten und Bindungen sind selbstredend nicht abgebildet. Diese zu identifizieren ist aber für die Compliance notwendig, da informelle Gruppen Kontrollmechanismen außer Kraft setzen und das Unternehmen gefährden (können).

Was sind informelle Gruppen?

Informelle Gruppen zeichnen sich durch direkte Beziehungen und physische Nähe der Mitglieder aus, die maximale Anzahl liegt bei 20 Mitgliedern. Die Mitglieder teilen Ziele und Werte und das eigene Handeln wird durch die anderen Mitglieder beeinflusst. Zudem ist die Zusammenarbeit meist dauerhaft.

Informelle Gruppen entwickeln zudem eigene Instrumente der Belohnung und Bestrafung. An erster Stelle steht die Zugehörigkeit bzw. der Status in der Gruppe. Mit gemeinsam begangen kriminellen Handlungen erhält die Gruppe darüber hinaus Sanktionsinstrumente. Wenn überführte Mitarbeiter mit strafrechtlicher Verfolgung und unverzüglicher Entlassung rechnen, ist die Sorge vor einer Aufdeckung besonders groß.

Unterschiedliche Risikoausprägung

Compliance-Verantwortliche sind daher darauf angewiesen, die Risikorelevanz einzelner Gruppen zu ermitteln, indem sie die unterschiedlichen Risikoausprägungen analysieren (siehe Tabelle).

Gruppenstruktur	Abteilungsübergreifend	hoch	gering
	Abteilungsintern	mittel	sehr hoch
		Dynamisch, Wachsend	Statisch, Schrumpfend
		Geschäftsfeldentwicklung	

- Gruppenstruktur

Abteilungsinterne Gruppen
Zu einer informellen Gruppe wird eine Abteilung, wenn die formellen Kriterien ausgeschaltet werden. Dies betrifft die Hierarchie, vor allem die Dienstaufsicht, zusätzlich werden Kontrollmechanismen einer Ebene, wie das „Vier-Augen-Prinzip" oder die Aufgabenrotation ausgesetzt.

Abteilungsübergreifende Gruppen
Abteilungsübergreifende Gruppen richten sich an bestimmten Prozessen aus. Wenn bspw. der Bedarfsanforderer Verwandter des Einkäufers ist, welcher wiederum einen Freund in der Rechnungsprüfung hat, werden Sicherheitsmaßnahmen unwirksam.

- Geschäftsfeldentwicklung

Schrumpfende Tätigkeitsfelder
Die Aufgaben sind nicht nur räumlich am Rand des Unternehmensgeländes angesiedelt. Die Tätigkeit ist wenig prestigeträchtig und unterdurchschnittlich bezahlt, die Personalbeschaffung ist schwierig, Gruppenmitglieder machen eigene Vorschläge.

Wachsende Tätigkeitsfelder
Aufgabenfelder oder Märkte geraten in den Blickpunkt, Wachstum ist das Motto. Schnelligkeit geht vor Sorgfalt, um Richtlinie und Vorschriften könne man sich nicht kümmern. Zwar kommen neue Mitarbeiter hinzu, die bei Beginn bereits tätigen Personen steigen gemeinsam auf und bleiben durch das alte Netzwerk einander verbunden.

Identifikation informeller Gruppen
Eine weitere Herausforderung besteht darin, die informellen Gruppen im Unternehmen zu identifizieren. Die folgenden Fragen geben Hinweise auf entsprechende Gruppen:

- In welchen Tätigkeitsfeldern besteht auffällig hohe oder geringe Fluktuation?
- Wer empfiehlt neue Mitarbeiter, wie erfolgt die Einstellung?
- Wann erfolgte der letzte Eintritt eines neuen Mitarbeiters?
- Haben die Mitarbeiter ihre Ausbildung in der gleichen Ausbildungsstätte absolviert?
- Gibt es verwandtschaftliche Beziehungen?
- Bestehen bei der überwiegenden Anzahl der Mitarbeiter vergleichbare Persönlichkeitsmerkmale: Geschlecht, Nationalität, Alter?
- Existieren unattraktive Aufgabenfelder? Resultieren daraus unterdurchschnittliche Bezahlung und geringe Aufstiegschancen?
- Sind Aufgabenfelder vom Unternehmensstammsitz räumlich getrennt?

Serie Mitarbeiter-Compliance
- Teil 1: Compliance: Ein Thema aller Mitarbeiter (http://www.compliancedigital.de/ce/compliance-ein-thema-aller-mitarbeiter/detail.html)
- Teil 2: Was Compliance-Verantwortliche von Geheimdiensten lernen können (http://www.compliancedigital.de/ce/was-compliance-verantwortliche-von-geheimdiensten-lernen-koennen/detail.html)
- Teil 3: Die Welt vor Compliance (http://www.compliancedigital.de/ce/die-welt-vor-compliance/detail.html)
- Teil 4: Einstieg ins Unternehmen (http://www.compliancedigital.de/ce/einstieg-ins-unternehmen-1/detail.html)
- Teil 5: Ausscheidende Mitarbeiter (http://www.compliancedigital.de/ce/ausscheidende-mitarbeiter/detail.html)
- Teil 6: Informelle Gruppen: Herausforderung für die Compliance

Im Teil 7 der Serie Mitarbeiter-Compliance erfahren Sie, was Sie gegen informelle Gruppen unternehmen können.

Zur Person
Dipl.-Kaufmann Thomas Schneider ist für die Corporate Compliance der Knauf Interfer SE verantwortlich, einem führenden Distributions-, Service- und Bearbeitungsunternehmen für Stahl und Aluminium. Er ist Verfasser zahlreicher Veröffentlichungen zur Compliance. Im Erich Schmidt Verlag ist der Band Mitarbeiter-Compliance erschienen.

Literaturhinweis
Weitere Informationen zu dem Thema gibt das Buch „Mitarbeiter Compliance (http://www.compliancedigital.de/ce/mitarbeiter-compliance/ebook.html)". Das eBook steht Abonnenten von COMPLIANCEdigital ebenfalls kostenfrei zur Verfügung.

Neues IPPF: Ein Anlass, die Rolle der Internen Revision im Unternehmen zu überprüfen

Nachricht vom 03.09.2015

Das IIA hat Mitte des Jahres das International Professional Practice Framework (IPPF) überarbeitet. Über die Änderungen und die Konsequenzen für die Interne Revision sprach die ESV-Redaktion mit Dr. Oliver Bungartz.

Warum war die Überarbeitung bzw. Ergänzung des IPPF notwendig?
Oliver Bungartz: Eine Überarbeitung des International Professional Practice Framework (IPPF) war nach einiger Zeit notwendig, um den neuen Entwicklungen und den geänderten Anforderungen im Bereich Interne Revision Rechnung zu tragen. Gesetzliche und regulatorische Anforderungen sowie Entwicklungen in den Bereichen Corporate Governance, Risikomanagement und Interne Kontrollsysteme (IKS) haben Anpassungen notwendig gemacht, damit die Interne Revision mit dem IPPF auf ein aktuelles Rahmenwerk zurückgreifen kann und um die gestiegenen Erwartungen erfüllen zu können. Unabhängig davon sollte jedes Rahmenwerk vor dem Hintergrund sich ständig verändernder Umfeldbedingungen in regelmäßigen Abständen überprüft und überarbeitet werden.

Was sind aus Ihrer Sicht die wesentlichen Änderungen?
Oliver Bungartz: Die wesentlichen Inhalte des IPPF, d. h. insbesondere die Definition der Internen Revision, der Ethikkodex, die „Internationalen Standards für die berufliche Praxis der Internen Revision (Standards)" sowie die Praktischen Ratschläge und Positionspapiere sind auch nach der Überarbeitung inhaltlich noch gültig.

Eine wesentliche Änderung ist die Einführung einer Mission und der Kernprinzipien einer Internen Revision als verbindliche Teile des IPPF. Darüber hinaus wurden die Praktischen Ratschläge als „Umsetzungsrichtlinien" (Implementation Guidance) und die Praxisleitfäden als „Unterstützende Leitlinie" (Supplemental Guidance) umstrukturiert.

Die Positionspapiere werden vom „The Institute of Internal Auditors (IIA)" weiterhin veröffentlicht, wurden aber als Komponente des IPPF herausgenommen, da sie eher als Hinweis für Interne Revisoren und Verlautbarungen mit Informationscharakter an Außenstehende gesehen werden und daher konsequenterweise nicht als Bestandteil des Rahmenwerks gelten müssen. Die Herausnahme der Positionspapiere als Komponente aus dem IPPF kann somit als folgerichtig beurteilt werden. Die einzelnen Bestandteile des IPPF werden jetzt in „vorgeschrieben" (d. h. Kernprinzipien, Definition, Standards und Ethikkodex) und „empfohlen" (d. h. Umsetzungsrichtlinien und Unterstützende Leitlinien) eingeteilt, um eine klare Abgrenzung vorzunehmen.

Wie bewerten Sie die Änderungen/Aktualisierungen? Reichen diese aus, um den Anforderungen der Revisoren in den nächsten Jahren gerecht zu werden?
Oliver Bungartz: Die Änderungen und Aktualisierungen können grundsätzlich als positiv und zielführend bewertet werden. Insbesondere durch die Einführung einer Mission und Kernprinzipien kann nun klar und prägnant beschrieben werden, was eine Interne Revision in einer Organisation erreichen möchte. Mission und Kernprinzipien können auch für die Kommunikation im Unternehmen sowie an externe Stakeholder genutzt werden, um verständlich zu beschreiben, welche Ziele, Aufgaben und Funktionen eine Interne Revision hat. Mit der Mission und den Kernprinzipien wird das Rahmenwerk sinnvoller Weise um strategische Aspekte einer Internen Revision ergänzt. Letztlich kann dies das Verständnis der Internen Revision von Außenstehenden erhöhen und das Image der Internen Revision verbessern.

Die neue Strukturierung des Rahmenwerks in „vorgeschriebene" und „empfohlene" Teile trägt zur Klarheit bei und konkretisiert die Anforderungen. Die Konzeption des Rahmenwerks lässt es zu, dass auch aktuelle Entwicklungen und Fragestellungen berücksichtigt werden können, um dem sich stetig verändernden Umfeld sowie den daraus resultierenden Anforderungen gerecht zu werden. Insgesamt waren die Änderungen notwendig, um ein modernes Rahmenwerk zu schaffen, welches auch zukünftige Entwicklungen und Veränderungen berücksichtigen kann.

Welche Auswirkungen sehen Sie auf die Rolle der Revision sowie auf die Revisionsprozesse? Wo müssen Unternehmen/Revisionsabteilungen nun aus ihrer Sicht am dringendsten nacharbeiten?
Oliver Bungartz: Die internen Revisionsabteilungen aller Organisationen sollten das neue IPPF als Anlass nehmen, ihre eigene Tätigkeit und Ausrichtung zu überprüfen und kritisch zu hinterfragen. Insbesondere kann die Einführung der Mission und Kernprinzipien – soweit noch nicht vorhanden – zu einer organisationsinternen Reform und Neuausrichtung der Internen Revision genutzt werden. Soweit die Interne Revision bislang das IPPF beachtet und gelebt hat, wird die Aktualisierung auf die tägliche Revisionsarbeit und die Revisionsprozesse keine große Auswirkungen haben, da die Definition, der Ethikkodex, die Standards und die Praktischen Ratschläge unverändert Gültigkeit behalten. Aber auch die Einhaltung dieser Vorgaben kann Teil der außerordentlichen Begutachtung der Internen Revision im Rahmen der Einführung des neuen IPPF sein. (ESV/ms)

Hinweis: Die aktuelle deutsche Fassung des IPPF können Sie hier (http://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2015_Standards_V3.pdf) herunterladen.

Kurzinformation:
Dr. Oliver Bungartz ist verantwortlich für den Bereich „Risk Advisory Services (RAS)" bei BRL – Boege Rohde Luebbehuesen und fachlicher Leiter des RAS-Bereichs bei RSM. Bei RSM ist Herr Dr. Bungartz verantwortlich für RAS in Deutschland und Kontinental-Europa. Schwerpunkte seiner Tätigkeit sind Dienstleistungen und Fortbildung in den Bereichen Interne Kontrollsysteme (IKS), Interne Revision, Risikomanagement, Compliance und Corporate Governance.
Im Erich Schmidt Verlag ist von Herrn Dr. Bungartz u. a. das Handbuch Interne Kontrollsysteme (IKS) (http://www.compliancedigital.de/ce/handbuch-interne-kontrollsysteme-iks-7/ebook.html) erschienen. Dr. Bungartz ist ebenfalls Herausgeber des „Lexikon Interne Revision (http://www.internerevisiondigital.de/lexikon.html)", welches Sie auf der Datenbank INTERNE REVISIONdigital finden.

Leutheusser-Schnarrenberger: Datenschutz auch für „rohe" oder „für sich belanglose" Daten

Nachricht vom 02.09.2015

Gesundheitsdaten sind heiß begehrt. Und mit den neuen Wearables liefern die Menschen diese Daten quasi umsonst. Über den Umgang und den Gefahren mit den Gesundheitsdaten sprach die Ping-Redaktion mit Sabine Leutheusser-Schnarrenberger.

Nicht erst seit der Apple Watch ist das Thema Gesundheitsdaten virulent. Für einen kurzen medialen Aufschrei sorgte aber dennoch die Ankündigung der Allgemeinen Ortskrankenkasse Nordost (AOK Nordost), den Kauf der dafür notwendigen Gadgets mit max. 50 Euro zu subventionieren.

An Apple a day keeps the Data away?
Das die AOK Nordost das nicht aus Barmherzigkeit für das wertvollste Unternehmen der Welt, Apple, tut ist klar. Vielmehr sollen die Nutzer dieser Gadgets zu einem gesünderen Lebensstil animiert werden, indem sie sich u. a. mehr bewegen oder gesünder ernähren. Mit Sensoren zur Schritt-, Kalorien- oder Herzfrequenzmessung, die in den sogenannten Wearables meist integriert sind und den entsprechenden Apps, können die Träger dieser kleinen Helfer ihre Aktivitäten kontrollieren, oder – um ein nicht so schönes Verb zu verwenden – überwachen. Doch was passiert mit den Bewegungsprofilen und gesammelten Messwerten? Ist es wirklich

sinnvoll, der Institution, die letztendlich für meine Arztrechnungen aufkommt, Zugriff auf derlei Daten zu ermöglichen? Und was passiert anschließend mit diesen Daten? Bleiben diese bei den Krankenkassen oder werden sie – wenn sich das Geschäftsmodell der Krankenkasse ändert – gewinnbringend weiter veräußert?

Erst denken, dann herunterladen

Die ehemalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) plädiert im Interview in der aktuellen Ausgabe (5/15) der Datenschutzzeitschrift PinG daher für einen sensibleren Umgang mit den eigenen Gesundheitsdaten.

Auch die Bundesdatenbeauftrage Andrea Voßhoff (CDU) steht dem Einsatz von Gesundheits-Apps kritisch gegenüber: „Allen Anwendern, die Fitness-Apps freiwillig herunterladen, rate ich, nicht unbedacht mit ihren sensiblen Gesundheitsdaten umzugehen und die kurzfristigen finanziellen Vorteile, welche die Datenoffenbarung vielleicht mit sich bringt, gegen die langfristigen Gefahren abzuwägen", so Voßhoff.

Medizinischer Fortschritt durch Big Data

In dem Interview plädiert die ehemalige Justizministerin allerdings auch dafür, dass Datenschutz nicht zum Hemmnis werden darf. Tumordatenbanken seien heutzutage unerlässlich, um eine bestmögliche Behandlung der Patienten zu gewährleisten. Aber: Gewebeproben zu Forschungszwecken sollten stets anonymisiert oder zumindest, mit entsprechender Sicherung, pseudonymisiert erhoben werden, so die Forderung Leutheusser-Schnarrenberger. Ihr Argument: „Auch mit anonymisierten Daten kann erfolgreiche Forschung betrieben werden."

Das gesamte PinG-Interview mit der ehemaligen Bundesjustizministerin lesen Sie hier (http://www.compliancedigital.de/ce/der-begriff-der-gesundheitsdaten-ist-weit-zu-fassen/detail.html).

Zur Person

Sabine Leutheusser-Schnarrenberger studierte Rechtswissenschaften in Göttingen und Bielefeld. Seit 1978 ist sie Mitglied der FDP und gehört dem Freiburger Kreis an. Von 1990 bis 2013 war die 64-jährige Juristin aus Minden Mitglied des Deutschen Bundestags. Bereits 1992 war sie Bundesjustizministerin, legte ihr Amt jedoch aus Widerstand gegen den „Großen Lauschangriff" 1996 nieder. Von 2009 bis 2013 war sie erneut Bundesjustizministerin. Bei Fragen zu Bürgerrechten und Datenschutz spielt sie eine wichtige Rolle. (ESV/ms mit Material von Ping, FAZ, BfDI)

Literaturhinweise zum Thema

Über aktuelle und grundlegende Fragen zum Datenschutz, informiert die Zeitschrift PinG – Privacy in Germany. Abonnenten von COMPLIANCEdigital lesen PinG (http://www.compliancedigital.de/short/ping/ejournal-inhalt.html) kostenfrei!

Know-how Schutz: Unter dem Compliance-Radar

Nachricht vom 24.08.2015

Die geplante Know-how-Schutz Richtlinie der EU steht vor der ersten Lesung im EU-Parlament im November. Ein Compliance-Thema? Ganz sicher!

Es gilt zunächst mit einem Missverständnis aufzuräumen: Beim „Kow-how-Schutz" geht es nicht um schutzfähige Güter wie patentfähige Erfindungen. Betroffen sind wertvolle, aber gerade nicht schutzfähige Assetts wie Kalkulationen, Kundenlisten, Konstruktionszeichnungen, Rezepte und, ja: sogar Ideen. Man mag also an die Rezeptur der Big-Mac-Sauce oder Coca-Cola denken. Hierzulande wohl auch aufgrund der Tatsache, dass der DAX von technologigetriebenen Unternehmen beherrscht wird, ist das Thema bislang eher vernachlässigt und unter dem „Compliance-Radar" verschwunden – trotz eines allgemeinen Lamentierens über die Folgen von Industriespionage.

Schutz von Know-how ist „lebensnotwendig"

Nun zeichnet sich ab, dass ein durchdachtes Know-how-Schutz-Konzept für viele Unternehmen mit der EU-weiten Vereinheitlichung des Rechts „lebensnotwendig" werden wird. Die EU-Kommission sah hier bereits vor Jahren Handlungsbedarf, weil die aktuellen Regeln der Mitgliedsländer zum Schutz von Geschäftsgeheimnissen und Know-how heillos zersplittert sind. Jetzt nehmen die Bestrebungen Fahrt auf: Der entsprechende Richtlinienentwurf zum Schutz vertraulichen Know-how und vertraulichen Geschäftsinformationen (COM 2013, 183) könnte schon zu Beginn des nächsten Jahres in Kraft treten.

Nach Verabschiedung der Richtlinie wird der Abfluss von Unternehmensinterna in den Wettbewerb oder die Öffentlichkeit rechtlich nur dann zu verteidigen sein, wenn die Informationen durch „angemessene Schutzmaßnahmen" fremdem Zugriff entzogen wurden. Das wird die Rechtslage hierzulande ändern: Denn bisher sieht die Rechtsprechung beim Geheimnisschutz eine Vermutung für einen Geheimhaltungswillen bei Unternehmen vor und stellt im Gesetz gegen den unlauteren Wettbewerb (UWG) keine hohen Anforderungen an den Geheimnisschutz.

Wie müssen sich Unternehmen schützen?

Doch was sind „angemessene Schutzmaßnahmen"? Gemeint ist ein Konzept, das die identifizierten, im Unternehmen sensiblen Informationen vor internem und externem Zugriff schützt – und zwar nicht nur tatsächlich, z. B. durch Zugangsbeschränkungen, sondern auch und vor allem rechtlich. Dazu zählen individuelle und konkrete Geheimhaltungsvereinbarungen, die in der bisherigen deutschen Praxis so gut wie nicht vorkommen.

Auswirkungen der EU-Richtlinie

Die Elemente eines solchen Schutzkonzepts müssen natürlich auf die Bedürfnisse des jeweiligen Unternehmens zugeschnitten werden. Eine rechtskonforme Umsetzung der Vorgaben, die die EU-Richtlinie vorgesehen hat, wird sich – in allen Branchen – jedenfalls in folgenden Bereichen auswirken:

- Vertragscompliance
  Bestehende und neue Verträge mit Mitarbeitern, Dienstleistern, Partnern und Kunden müssen auf den Prüfstand. Bisherige pauschale „Vertraulichkeitsvereinbarungen/NDAs" werden vor dem Hintergrund der Richtlinie keinen Bestand mehr haben. Betriebsgeheimnisse werden in Zukunft konkret bezeichnet werden müssen, um ein Minimum an wettbewerbsrechtlichem Schutz zu erreichen.

Auch die üblichen Klauseln in Verträgen mit Arbeitnehmern, die sich auch nach dem Ausscheiden zur Verschwiegenheit verpflichten, sind – wenn nicht bereits nach geltendem Recht – spätestens mit Umsetzung der Richtlinie wettbewerbsrechtlich wertlos. Auch hier werden Unternehmen nicht umhinkommen, Wissensträger zu identifizieren und vertraglich zur Geheimhaltung über konkret bezeichnete Geheimnisse zu verpflichten.

- Ermittlung und Klassifizierung des Know-hows
  Eine Herausforderung für das Informationsmanagements im Unternehmen wird es sein, nicht nur zu prüfen, ob Informationen oder Innovationen schutzrechtsfähig (z.B. Patente) sind. Unternehmensgeheimnisse müssen vielmehr selbständig bewertet und klassifiziert werden. Damit einher gehen Berechtigungen der Mitarbeiter beim Zugang zu diesen Geheimnissen (und zwar nicht nur auf IT-Ebene).
- Rechtsdurchsetzung
  Über die Einhaltung eines den EU-Vorgaben genügenden Know-how-Schutzsystems werden Unternehmen genau wachen müssen: Nur wer den Abfluss von Know-how an Dritte bemerkt und sich dagegen wendet, verhilft den Unternehmensinteressen zum Durchbruch. Dazu gehört die Überwachung, Abmahnung und gegebenenfalls gerichtliche Inanspruchnahme von Wettbewerbern, die sich der Informationen eines Konkurrenzunternehmens bemächtigt haben.

Unter Compliance-Gesichtspunkten wird die Umsetzung der Vorgaben aus der EU-Richtlinie kein kurzfristiges Projekt sein. Sie erfordert eine Sensibilisierung der Mitarbeiter, bietet gleichzeitig aber auch die Chance die Zusammenarbeit zwischen Rechts- und Complianceabteilungen mit den Fachabteilungen zu vertiefen und Geheimnisse dadurch effektiv zu schützen. Es gilt: Was der Wettbewerber nicht kennt, kann er auch nicht kopieren.

Informationen zum Autor:
David Ziegelmayer (http://www.cms-hs.com/david-ziegelmayer) ist Rechtsanwalt bei der Kanzlei CMS Hasche Sigle in Köln. Er ist als Fachanwalt für gewerblichen Rechtsschutz spezialisiert auf den Schutz von Know-how- und Reputation von Unternehmen.

Compliance hat noch Luft nach oben

Nachricht vom 19.08.2015

Viele Unternehmen halten Compliance zwar für wichtig. Allerdings halten nur 50 Prozent von ihnen ein Compliance-Schulungsprogramm vor, so das Ergebnis des aktuellen Compliance-Barometers von CMS Hasche Sigle.

Dass Compliance eine immer größere Rolle in den Unternehmen gewinnt, ist unbestritten – auch, wenn es noch Luft nach oben in Sachen Professionalisierung gibt, wie die aktuelle Studie „CMS – Compliance Barometer" von der Wirtschaftskanzlei CMS Hasche Sigle gerade gezeigt hat (Siehe hierzu auch den Beitrag „Compliance: Gekommen um zu bleiben (http://www.compliancedigital.de/ce/compliance-gekommen-um-zu-bleiben/detail.html)" vom 17.08.2015).

Vor allem das gesteigerte Risikobewusstsein in den Unternehmen und bei den verantwortlichen Führungskräften zwingt die Firmen dazu, die Compliance-Systeme weiter zu professionalisieren. Während in Konzernen vor allem Korruptions- und Kartellrechtsverstöße ganz oben auf der Risiko-Agenda stehen, beschäftigt den größeren Mittelstand vor allem das Thema Datenschutz, so das Ergebnis der Umfrage unter 175 großen Unternehmen (http://www.compliancedigital.de/ce/compliance-gekommen-um-zu-bleiben/detail.html).

Compliance-Anforderungen wachsen
Doch nicht nur veränderte Risikoeinschätzungen lassen Unternehmen in Sachen Compliance handeln. Auch steigende Haftungsmaßstäbe durch die zunehmende Regulierung der Gesetzgebung und die strengere Praxis von Behörden und Rechtsprechung führen in den Augen der Befragten dazu, dass die Compliance-Anforderungen an die Unternehmen immer weiter zunehmen, mit der Folge, dass der Handlungsdruck weiter steige.

Zudem müssen Unternehmen gegenüber ihren Geschäftspartnern – und Vice versa – immer öfter nachweisen, dass sie ein funktionierendes Compliance-Management-System vorhalten (http://www.compliancedigital.de/ce/ist-mein-geschaeftspartner-compliant/detail.html). In der CMS Hasche Sigle-Umfrage gaben über die Hälfte der Befragten deshalb an, dass es für sie wichtig sei, ein solches nachweisen zu können.

Herausforderung: Compliance-Kultur
Eine entscheidende Rolle bei all den Bemühungen, die Compliance in den Unternehmen zu verbessern, spielt die Unternehmenskultur. Fast drei Viertel der Befragten gab an, dass die größte Herausforderung darin bestehe, bei Mitarbeitern wie bei der Unternehmensleitung ein echtes Bewusstsein und eine Akzeptanz für die Thematik zu etablieren – Stichwort Mitarbeiter-Compliance (http://www.compliancedigital.de/contenttyp_title_plural/News/q/Mitarbeiter-Compliance/suche.html). Während 88 Prozent dem Management ein hohes Compliance-Bewusstsein bescheinigen, ist bei den restlichen Mitarbeitern nur ein Drittel dieser Auffassung. Und während fast alle Unternehmen mittlerweile über grundlegende Compliance-Instrumente verfügen, hat lediglich die Hälfte der befragten Unternehmen ein Compliance-Schulungsprogramm zur Vermittlung von Verhaltensanforderungen. Auch hier gilt: Es gibt noch Luft nach oben! (ESV/ms mit Material von CMS Hasche Sigle)

Literaturempfehlung Mitarbeiter-Compliance
Wie erreiche ich die Mitarbeiter mit dem Thema Compliance? Thomas Schneider und Maike Becker zeigen in dem Band Mitarbeiter-Compliance (http://www.compliancedigital.de/ce/mitarbeiter-compliance/ebook.html) Strategien auf, wie Compliance Thema aller Mitarbeiter werden kann.

Compliance: Gekommen um zu bleiben

Nachricht vom 17.08.2015

Wie hältst Du es mit der Compliance? Diese Frage stellte die Wirtschaftskanzlei CMS Hasche Sigle den großen deutschen Unternehmen. Die Antwort: Compliance ja – aber noch nicht so richtig. Vor allem KMU haben Nachholbedarf.

Zwar sei Compliance mittlerweile in Unternehmen fest verankert (http://www.compliancedigital.de/ce/compliance-mehr-als-eine-welle/detail.html), so das Ergebnis der ersten branchenübergreifenden Studie „CMS Compliance Barometer (http://www.cms-hs.com/PM_CMS_Compliance-Barometer_11_08_2015)"

von CMS Hasche Sigle – allerdings gebe es noch Luft nach oben. Insgesamt, so das Fazit der Studie, sei das Thema Compliance noch nicht ausreichend professionalisiert. Für die Studie wurden Compliance-Verantwortliche aus 175 großen Unternehmen (mindestens 500 Mitarbeiter) anonym und repräsentativ vom Marktforschungsinstitut Ipsos befragt.

Regulierung und hohe Risiken sind Treiber für Compliance

Dass Compliance in den Unternehmen angekommen ist, darüber bestehen kaum Zweifel. Immer mehr Regulierungspflichten und steigende Risiken für Unternehmen, aber auch für die Mitarbeiter persönlich, die aus einem unzureichenden Compliance-Management entstehen können, sind Gründe, dass Compliance inzwischen eine anerkannte Funktion in den Unternehmen ist, so Dr. Harald W. Potinecke, Partner und Koordinator der deutschen Compliance-Gruppe bei CMS. Zudem sei das Thema Compliance auch beim großen Mittelstand angekommen und nicht länger mehr nur ein Thema der international operierenden Konzerne, so Potinecke.

Professionalisierung von Compliance weiter ausbaubar

Allerdings gebe es – mit Blick auf die Studienergebnisse – noch Professionalisierungsreserven. Zwar wurden in fast der Hälfte der befragten Unternehmen in den vergangenen Jahren die finanziellen als auch die personellen Kapazitäten aufgestockt. Andererseits verfügt nur ein Drittel über eine eigenständige Compliance-Abteilung. Diese sind zudem meist in der Rechtsabteilung, im Controlling, im Risikomanagement oder in der Revision angesiedelt.

Überdies sind die Abteilungen immer noch sehr übersichtlich, was die personelle Ausstattung anbelangt. In der Regel beschäftigen sich ein bis vier Mitarbeiter mit Compliance-Fragen – und das oftmals noch nicht einmal primär. Häufig müssen die Mitarbeiter weitere Aufgaben übernehmen.

Aus Sicht der Studienautoren von CMS Hasche Sigle ist vor allem problematisch, dass bei fast einem Drittel der Unternehmen Mitarbeiter aus Vertrieb und Einkauf Compliance-Funktionen ausüben. Hier können, so Dr. Tobias Teicke, Compliance-Experte am CMS-Standort Berlin, „Haftungsrisiken drohen, wenn operatives Risikogeschäft und Compliance-Verantwortlichkeiten nicht klar getrennt voneinander gemanagt werden".

Auch werden die oftmals bescheidenden Compliance-Ressourcen unzureichend genutzt: In etwa jedem zweiten Unternehmen sind bestehende Abteilungen nicht optimal miteinander verzahnt. Weit verbreitet sei dagegen die Praxis, extern fachliche Unterstützung einzuholen. Je nach Compliance-Thema liege die Beratungsquote bei bis zu 80 Prozent, so Teicke.

Unterschiedliche Risikoeinschätzung zwischen KMU und Konzernen

Auch die Risikoeinschätzung in vielen Unternehmen überraschte die Experten von CMS Hasche Sigle. Demnach spielen kartellrechtliche Fragen (http://www.compliancedigital.de/ce/kartellrechts-compliance-auch-fuer-kmu/detail.html) und Korruption für mittelständische Unternehmen nur eine untergeordnete Rolle. Als weitaus wichtiger wird dagegen das Thema Datenschutz (http://www.compliancedigital.de/ce/cyber-attacken-sind-genauso-wenig-vorhersagbar-wie-erdbeben/detail.html) genommen – was sicherlich auch mit der intensiven Berichterstattung zu tun hat. In Großunternehmen wiederum werden hingegen Korruptions- und Kartellrechtsverstöße und die damit verbundenen Strafzahlungen als Hauptrisiko eingeschätzt. Die unterschiedliche Risikoeinschätzung spiegele die bei gerade mittelständischen Unternehmen immer noch weit verbreitete Auffassung wider, Korruption käme bei ihnen nicht vor, so Florian Block, Compliance-Experte am Münchener CMS-Standort. Dies sei – angesichts der bekanntgewordenen Fälle – jedoch ein Trugschluss (http://www.compliancedigital.de/ce/kartellrechts-compliance-auch-fuer-kmu/detail.html). (ESV/ms mit Material von CMS Hasche Sigle)

Literaturempfehlung zum Thema Compliance

In der aktuellen Ausgabe der Zeitschrift für Corporate Governance (ZCG 4/15) befasst sich Prof. Dr. Harald Ehlers in seinem Beitrag „Kartellrechts-Compliance (http://www.compliancedigital.de/ce/kartellrechts-compliance-auch-fuer-kmu-notwendig/detail.html)" mit dem Stellenwert von Kartellrechts-Compliance in KMU.

Einen umfassenden Überblick über das Thema Compliance bietet das von Prof. Dr. Josef Wieland, Dr. Roland Steinmeyer und Prof. Dr. Stephan Grüninger herausgegebene „Handbuch Compliance-Management (http://www.compliancedigital.de/ce/handbuch-compliance-management-2/ebook.html)". In dem Handbuch setzt sich Dr. Georg Weidenbach mit der Frage der existenzsichernden Bedeutung von Compliance im Kartellrecht (http://www.compliancedigital.de/ce/die-existenzsichernde-bedeutung-von-compliance-im-kartellrecht-1/detail.html) auseinander.

Und welche kartellrechtlichen Vorgaben und Verpflichtungen notwendig sind, finden Sie in der gleichnamigen Arbeitshilfe (http://www.compliancedigital.de/ce/kartellrechtliche-vorgaben-und-verpflichtungen/detail.html) von Prof. Dr. Stefan Behringer.

Kartellrechts-Compliance – auch für KMU

Nachricht vom 14.08.2015

Wie können kartellrechtliche Gefahrenlagen abgewendet werden? Ein Praxisbericht von Prof. Ehlers von der FH-Kiel zeigt Wege auf, was KMU gegen Kartellrechtverstöße unternehmen können.

In den letzten Jahren flogen eine Vielzahl von Kartellen auf. Betroffen waren hier meist größere Konzerne. Doch auch kleine und mittlere Unternehmen (KMU) rücken verstärkt in den Fokus der Kartellbehörden, erklärt Prof. Dr. Harald Ehlers von der Fachhochschule Kiel in einem Beitrag für die Zeitschrift Corporate Governance – ZCG (Ausgabe: 4/15) (http://www.compliancedigital.de/ce/kartellrechts-compliance-auch-fuer-kmu-notwendig/detail.html).

Es geht um mehr als Wurst und Zucker

So hat die Kartellbehörde im Juli 2014 gegen 21 Wursthersteller ein Bußgeld von insgesamt rund 338 Millionen Euro verhängt. Im gleichen Jahr mussten die drei größten deutschen Zuckerhersteller rund 280 Millionen Euro an Strafe zahlen. Und der Druck auf die Kartelle hält weiter an. Das Bundeskartellamt schließt heute dreimal so viele Verfahren ab, wie dies noch Mitte der 90er Jahre – Tendenz steigend. Kein Wunder also, dass die Summe der verhängten Bußgelder im Jahr 2014 erstmals die Schallmauer von einer Milliarde Euro durchbrochen hat (http://www.compliancedigital.de/ce/2014-das-jahr-der-kartellbussen/detail.html).

Und auch Unternehmen kämpfen verstärkt gegen Kartelle an – allen voran die Deutsche Bahn (http://www.compliancedigital.de/ce/bahn-macht-gegen-kartelle-mobil/detail.html), sind sie es doch, die am meisten unter den Kartellen durch Marktverzerrungen und überhöhten Preisen leiden.

Wirksame Instrumente gegen Kartelle
Neben einem gewachsenen Problembewusstsein sowohl in Politik, Öffentlichkeit und auch in den Unternehmen selbst, kann das Bundeskartellamt auf wirkungsvolle Instrumente zurückgreifen, welche die Aufdeckung von Kartellen erleichtert. Dazu zählen beispielsweise die Sektor-Untersuchungen auf Basis der 7. GWB-Novelle aus dem Jahr 2005, der Bonus- und Kronzeugenregelungen oder aber auch durch eine verbesserte grenzüberschreitende Zusammenarbeit im Rahmen des European Competition Network – dem Netzwerk der EU-Wettbewerbsbehörden.

Compliance gegen Schutz vor Kartellen
Unternehmen müssen – wollen sie nicht in die Gefahr von hohen Strafzahlungen, Ausschluss von Aufträgen oder Privatklagen geraten – in wirksame Kartellrechts-Compliance-Management-Systeme (CMS) investieren.

Die Anforderungen an Kartellrechts-CMS sind dabei nicht trivial. Die Systeme müssen

- den Mitarbeitern Kenntnis über das Kartellrecht und über die Risiken bei Kartellrechtverstößen vermitteln;
- die Mitarbeiter von kartellrechtswidrigen Verhalten abschrecken;
- Verstöße rechtzeitig aufdecken und zwar bevor es zu einer Untersuchung durch die Behörden kommt;
- Bußgelder gänzlich durch Vermeidung von Kartellrechtsverstößen ausschließen oder dadurch verhindern, dass ein funktionierendes Compliance-Programm nachgewiesen wird;
- das Risiko von Schadensersatzklagen und Rufschäden zu vermeiden.

Um diesen Anforderungen Genüge zu tun, müssen die Systeme nach Auffassung von Prof. Ehlers, folgerichtig

- ein ausdrückliches, schriftlich dokumentiertes und allen Mitarbeitern kommuniziertes Bekenntnis der Geschäftsführung zur Beachtung des Kartellrechts enthalten,
- eine Identifizierung der kartellrechtsrelevanten Risikobereiche im Unternehmen gewährleisten,
- eine kartellrechtliche Schulung der Mitarbeiter beinhalten,
- entsprechende schriftliche Verhaltensweisen vorhalten und
- eine permanente Kontrolle, insbesondere der Rechtsänderungen, sicherstellen.

Literaturempfehlung zum Thema Kartellrechts-Compliance
Den gesamten Beitrag „Kartellrechts-Compliance: Auch für KMU notwendig (http://www.compliancedigital.de/ce/kartellrechts-compliance-auch-fuer-kmu-notwendig/detail.html)“ von Prof. Ehlers können Sie in der aktuellen Ausgabe der Zeitschrift für Corporate Governance (ZCG 4/15) nachlesen.
In dem von Prof. Dr. Josef Wieland, Dr. Roland Steinmeyer und Prof. Dr. Stephan Grüninger herausgegebenen „Handbuch Compliance-Management“ setzt sich Dr. Georg Weidenbach in seinem Beitrag mit der existenzsichernden Bedeutung von Compliance im Kartellrecht (http://www.compliancedigital.de/ce/die-existenzsichernde-bedeutung-von-compliance-im-kartellrecht-1/detail.html) auseinander.
Welche Kartellrechtliche Vorgaben und Verpflichtungen notwendig sind, finden Sie in der gleichnamigen Arbeitshilfe (http://www.compliancedigital.de/ce/kartellrechtliche-vorgaben-und-verpflichtungen/detail.html) von Prof. Dr. Stefan Behringer.

Compliance: Mehr als eine Welle?

Nachricht vom 13.08.2015

Ist Compliance nur eine Welle, die bald vorüber geht? Warum die Gegenrevolution ausbleibt, erklärt Prof. Dr. Leonhard Knoll von der Universität Würzburg in der aktuellen Ausgabe der ZRFC.

Compliance: Was vor ein paar Jahren noch bei den meisten ein Achselzucken und bei einigen kritischen Zeitgeistern höchstens ein verzagtes Stirnrunzeln hervorgerufen hat, lockt heute – wenn auch längst nicht bei jedem (http://www.compliancedigital.de/ce/compliance-ein-thema-aller-mitarbeiter/detail.html) – zumindest ein wissendes Nicken hervor. Und von denjenigen, die damals skeptisch dem neumodischen englischen Begriff gegenüber standen, wünscht sich heute bestimmt ein nicht kleiner Teil, dass die Compliance-Welle bald auch wieder vorüber geht. Das Gegenteil ist der Fall – oder, wie Prof. Dr. Leonhard Knoll in seinem aktuellen Beitrag „Zum Hintergrund der Compliance-Welle: Wissenschaftler und Aufsichtsräte als Spiegel einer gesellschaftlichen Entwicklung (http://www.compliancedigital.de/ce/zum-hintergrund-der-compliance-welle/detail.html)“ für die ZRFC (4/15) beschreibt –: Die „Gegenrevolution“ finde nicht statt.

Compliance bleibt uns erhalten
Was sind die Gründe hierfür? Das Compliance mittlerweile auf der Agenda ganz oben steht, hat mit einer Vielzahl von Skandalen in der Vergangenheit zu tun. Zum Turnaround kam es aber vor allem durch die Lehman-Pleite und deren Folgen. Die wahren Gründe, warum Compliance mehr ist als eine Modeerscheinung, liegen viel tiefer, so Knoll.

1. Verlust der homogenen Strukturen
Das Ende des Kommunismus Anfang der 90er Jahre war zugleich der Beginn des Siegeszuges der Globalisierung. Eine Folge – so Knoll – ist, dass immer mehr Menschen mit unterschiedlichsten Hinter- oder Vordergründen aufeinandertreffen – Stichwort Diversity. Ein einheitlicher Wertekanon – falls so einer jemals existiert hat – kann nicht mehr vorausgesetzt werden. Dementsprechend können einheitliche Werte auch nicht ohne weiteres durchgesetzt werden. Ergo: Es bedarf Regeln, die letztendlich auch mit Sanktionen durchzusetzen sind.

2. Moderne Informations- und Kommunikationstechnologien
Ein weitere Folge – oder vielleicht auch die Ursache – der Globalisierung, sind die neuen Kommunikationsmöglichkeiten. War es früher noch eher möglich, gewisse Geheimnisse für sich zu behalten und Skandale unter den berühmten Teppich zu kehren, ist es heute – zum Glück – nicht mehr so leicht möglich. Whistleblower, wie der US-amerikanische Geheimdienstmitarbeiter Edward Snowden, sind in der Lage, selbst den „besten“ Geheimdienst und damit auch die ihm tragende Nation bloß zu stellen. Das gleiche gilt

auch für Unternehmen. Keine Organisation kann sich mehr sicher sein, dass kriminelle Machenschaften, egal wo auf der Welt, irgendwann auffliegen werden. Und das gilt nicht nur für die eigene Firma, sondern auch für die Geschäftspartner.

3. Schwindende Ehrfurcht vor bestimmten Personengruppen
Damit verbunden ist auch eine Abnahme von Respekt und Ehrfurcht vor gewissen Personengruppen. Das Bild des „ehrbaren Kaufmanns" oder des fürsorglichen Politikers hat in den vergangen Jahren sehr gelitten – und teilweise auch zu recht.

Die öffentliche Kontrolle – nicht zuletzt auch dank der neuen Kommunikationsmittel – führt dazu, dass (fast) niemand mehr über dem Gesetz steht – zumindest in den meisten OECD-Ländern.

4. Steigender Einfluss von internationalen Wirtschaftskanzleien
Ein letzter Grund, warum Compliance keine Modeerscheinung ist, die bald vorüber geht, ist der wachsende Einfluss internationaler Wirtschaftskanzleien und damit einhergehend die Etablierung und Durchsetzung entsprechender Kodizes.

Den gesamten Beitrag von Prof. Knoll (http://www.compliancedigital.de/ce/zum-hintergrund-der-compliance-welle/detail.html) können Sie in der aktuellen Ausgabe der Zeitschrift für Risk, Fraud & Compliance (ZRFC 4/15) nachlesen.

Weitere Beiträge der aktuellen Ausgabe sind:

- Streitgespräch zum Thema Compliance und CMS (http://www.compliancedigital.de/ce/streitgespraech-zum-thema-compliance-und-cms/detail.html) (Dr. Tatjana Aigner-Hof, Prof. Dr. Axel Halfmeier, Prof. Dr. Hagen Hof)
- The Business Case to Counter Corruption in India: Eine Umfrage unter Führungskräften zu Chancen und Herausforderungen von Korruptionsprävention in Indien (http://www.compliancedigital.de/ce/the-business-case-to-counter-corruption-in-india/detail.html) (Florian Lair)
- IDW PS 980 – Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen: Eine Einführung in die Grundlagen des Prüfungsstandards (http://www.compliancedigital.de/ce/idw-ps-980-grundsaetze-ordnungsmaessiger-pruefung-von-compliance-management-systemen/detail.html) (Dr. Karl-Heinz Withus)
- Compliance-Schulung für Unternehmenseinsteiger: Ein Fallbeispiel (http://www.compliancedigital.de/ce/compliance-schulung-fuer-unternehmenseinsteiger/detail.html) (Thomas Schneider)

Mehr IT-Sicherheit für Behörden

Nachricht vom 07.08.2015

IT-Sicherheit ist das Zukunftsthema für Behörden, so der Branchenkompass Public Service 2015 von Sopra Steria Consulting. Doch nicht nur Behörden sind gefordert. IT-Sicherheit ist längst eine gesamtgesellschaftliche Aufgabe.

Just, als der Bundestag das IT-Sicherheitsgesetz verabschiedet hat, kämpfte die Bundestags-IT-Abteilung gerade mit dem größten Angriff auf ihr IT-Netzwerk. Unbekannte – vermutlich aber ein ausländischer Geheimdienst – haben versucht, in das interne Datennetz des Bundestages einzudringen (http://www.compliancedigital.de/ce/cyber-attacken-sind-genauso-wenig-vorhersagbar-wie-erdbeben/detail.html) . Die Konsequenz: Mitte August werden zentrale Komponenten des IT-Systems abgeschaltet und neu aufgesetzt. Die Abgeordneten des „Land der Ideen" sind damit vier Tage quasi von der Welt abgeschnitten.

IT-Sicherheit ist zentrales Zukunftsthema
Doch nicht nur der Bundestag kämpft mit den Folgen der wachsenden Bedrohung aus dem Netz. „Viele Behörden erkennen das Thema IT-Sicherheit als ein zentrales Zukunftsthema und sehen hier weiteren Investitionsbedarf", so Olaf Janßen, der IT-Sicherheitsexperte von Sopra Steria Consulting und Autor des aktuellen „Branchenkompass Public Service 2015". Die angespannte Haushaltssituation und der hohe Bedarf an IT-Sicherheitsexperten stellen viele Behördenleiter aber vor große Herausforderungen, so Janßen weiter.

Behörden investieren in IT-Sicherheit
Der Branchenkompass zeigt aber auch, dass die Behörden das Thema – trotz der angespannten Haushalte und des Personalmangels – bereits angehen.

Neun von zehn der Befragten Entscheider aus 100 deutschen Bundes-, Landes- und Kommunalverwaltungen gaben an, dass ihre Behörden bereits in die IT-Sicherheit investieren. Zudem seien neue Investitionen bereits fest eingeplant, da die Verwaltungen auf ein zielgerichtetes und effizientes IT-System drängen. Auch rechtlich sind die Behörden durch den Umsetzungsplan Bund (UP Bund) verpflichtet, den IT-Grundschutz in den Behörden sicherzustellen.

IT-Sicherheit als gesamtgesellschaftliche Aufgabe
Neben Behörden müssen aber auch Unternehmen und andere Institutionen in die IT-Sicherheit investieren. Auch die Aufsichtsbehörden haben hier Nachholbedarf. Nach Ansicht von Dr. Hans Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz ist der „Schutz hochsensibler Informationen und kritischer Infrastrukturen zu einer vorrangigen Aufgabe der Sicherheitsbehörden geworden". Es bedarf daher, so Maaßen in dem Beitrag „Cyberwar – eine reale Gefahr aus der virtuellen Welt" für die Datenschutz-Fachzeitschrift PinG, einer „umfassenden, gesamtgesellschaftlichen Strategie", um Cyberwar, -Spionage und Infokrieg entgegenzuwirken. Abwehrmöglichkeiten müssten optimiert werden – technisch, rechtlich und analytisch.

Maaßen: IT-Sicherheitsgesetz ist ein „Meilenstein"
Integraler Bestandteil der Maßnahmen ist das seit Juli in Kraft getretene IT-Sicherheitsgesetz. Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist in den Augen von Maaßen ein „Meilenstein" (http://www.compliancedigital.de/ce/cyberrisiken-nehmen-zu-die-abwehr-aber-auch/detail.html) .

Literaturempfehlung zum Thema Datensicherheit
Seit kurzem steht die Zeitschrift Privacy in Germany (PinG) (http://www.compliancedigital.de/short/ping/ejournal-inhalt.html) Abonnenten von COMPLIANCEdigital kostenfrei zur Verfügung. In der aktuellen Ausgabe (4/2015) gehen die Autoren der Frage nach, wie die richtige Balance zwischen

Freiheit und Sicherheit in einem Rechtstaat gefunden werden kann?

Der neue DIIR-Praxisleitfaden „Revision von IT-Verfahren in öffentlichen Institutionen (http://www.compliancedigital.de/ce/revision-von-it-verfahren-in-oeffentlichen-institutionen/ebook.html)“ setzt sich konkret mit der Frage des Datenschutzes in Behörden auseinander. Grundlegend beschreiben die Experten der Fachgruppe „ERP in öffentlichen Institutionen“, wie Ämter die Prüfungen von IT-Verfahren effizient gestalten können.

Wie Unternehmen wesentliche regulatorische Anforderungen an die IT identifizieren, priorisieren und deren Erfüllung einer effizienten Steuerung zuführen, erläutern Michael Rath und Rainer Sponholz in dem Band „IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen (http://www.compliancedigital.de/ce/it-compliance-7/ebook.html)“.

Eine praxisorientierte Einführung in die Welt der IT-Prüfung bietet Stefan Beißel in dem Band „IT-Audit: Grundlagen – Prüfungsprozess – Best Practice (http://www.compliancedigital.de/ce/it-audit/ebook.html)“. Anhand eines umfassenden Prüfungskatalogs können Sie systematisch erschließen, worauf es bei der Vorbereitung, der Durchführung und dem Abschluss erfolgreicher IT-Audits ankommt.

Pofalla neuer Compliance-Vorstand bei der Bahn

Nachricht vom 29.07.2015

Ronald Pofalla wird neuer Compliance-Vorstand bei der Deutschen Bahn. Noch als Kanzleramtsminister hat er eine stärkere Regulierung der Bahn verhindert.

Lange Zeit wurde darüber spekuliert – nun ist es amtlich. Ronald Pofalla (CDU) – ehemaliger Kanzleramtsminister wird Vorstand bei der Deutschen Bahn (DB). Zukünftig verantwortet er das neu geschaffene Ressort Wirtschaft, Recht und Regulierung. In dieser Funktion wird er auch für die Compliance für die Deutsche Bahn Verantwortung tragen.

Pofalla löst Gerd Becht ab

Der Wechsel von Pofalla an die Konzernspitze bedeutet zugleich das Aus für Gerd Becht. Der Jurist Becht wurde 2009 als Vorstand Compliance, Datenschutz, Recht und Konzernsicherheit berufen. Unter der Ägide von Becht „wurde das durch die Datenaffäre massiv verlorene Vertrauen der Belegschaft zurückgewonnen“, so der Vorsitzende des Aufsichtsrates, Prof. Dr. Dr. Utz-Hellmuth Felcht. Heute setze die Bahn beim Datenschutz und mit ihrer hochprofessionellen Compliance-Organisation deutschlandweit Maßstäbe, so Felcht weiter.

Zudem habe Becht bei der Verfolgung ziviler Rechtsansprüche exzellente Ergebnisse erzielt, so der Deutsche Bahn Vorstandsvorsitzende Dr. Rüdiger Grube: „Beispielsweise gelang es ihm und seinem Team, im Rahmen des Schienen- oder Rolltreppenkartells hunderte Millionen Euro Schadenersatz für die DB und auch die Steuerzahler zu erwirken.“ (siehe hierzu auf die Meldung auf COMPLIANCEdigital vom 01.09.2014 (http://www.compliance-digital.de/ce/bahn-kaempft-erfolgreich-gegen-kartelle/detail.html))

Ist der Wechsel compliant?

Im Vorfeld gab es hinsichtlich des geplanten Wechsels von Pofalla an die Bahnspitze Kritik, nicht nur von der Opposition. In den Augen von Staatsrechtler Hans Herbert von Arnim handele es sich hier um „eine Form der bezahlten Korruption“. Das Vorgehen, so Armin in der FAZ im Januar 2014, begründe den Verdacht der Interessenkollision, denn Pofalla könne schon in seinem politischen Amt die Interessen seines künftigen Arbeitgebers mit im Blick gehabt haben.

Gegenüber der ARD kritisierte der Fraktionsvorsitzende der Grünen im Bundestag, Anton Hofreiter, den Wechsel ebenfalls scharf: „Selbstverständlich hat jemand das Recht, aus der Politik in der Wirtschaft Karriere zu machen.“

Konkret kritisierte Hofreiter damals, dass Pofalla als Kanzleramtsminister unter anderem beim Eisenbahn-Regulierungsgesetz eine stärkere Kontrolle der Bahn verhindert habe. „Man kann sagen, wenn man hart sein will, dass dies eine nachgelagerte Belohnung ist; dass dies im Grunde genommen fast eine Form von Korruption ist, für Entscheidungen, die er getroffen hat, als er Kanzleramtsminister war“, so Hofreiter gegenüber der ARD.

Karenzzeit für Politiker

Nicht zuletzt der Fall Pofalla führte bei der Bundesregierung zur Einsicht, den Übergang von Politikern in die Wirtschaft zu regeln. Im Februar dieses Jahres hat das Bundeskabinett für aktuelle und frühere Minister und parlamentarische Staatssekretäre eine Auszeit von mindestens zwölf Monaten beschlossen. Diese Frist gelte, bevor die Betroffenen einen bezahlten Job oder eine andere Beschäftigung außerhalb des öffentlichen Dienstes annehmen. Bei Interessenskonflikten kann die Bundesregierung – so der Vorschlag – die Frist auf 18 Monate erhöhen.

Aus Sicht der Organisationen LobbyControl und Transparency International Deutschland e.V. ist der Gesetzentwurf allerdings ungenügend. Zwar sei die gesetzliche Regelung zu begrüßen, doch sehen beide Organisationen die Länge der Karenzzeit und das Fehlen von Sanktionen bei Verstößen kritisch. Zudem fordern sie ein generelles Verbot, während der Karenzzeit eine Lobbytätigkeit in der Wirtschaft anzunehmen. (Quellen: Deutsche Bahn, Tageschau, FAZ, Transparency International Deutschland)

Grundlagenliteratur zu Compliance

Das Management von Compliance und Integrität ist heute wesentliche Aufgabe erfolgreicher Unternehmensführung. Erst die Sicherstellung eines rechtlich einwandfreien, gesellschaftlich akzeptablen und betriebswirtschaftlich effizienten Unternehmenshandelns garantiert nachhaltig Marktzugang, Wertschöpfung und Wohlstand. Welche Mindestanforderungen ein zielgerichtetes Compliance-Management in Wirtschaft und Verwaltung heute erfüllen muss, um glaubwürdig, effizient und effektiv zu sein, erläutern die Autoren rund um die Herausgeber Prof. Dr. Josef Wieland, Dr. Roland Steinmeyer und Prof. Dr. Stephan Grüninger im „Handbuch Compliance-Management: Konzeptionelle Grundlagen, praktische Erfolgsfaktoren, globale Herausforderungen (http://www.compliancedigital.de/ce/handbuch-compliance-management-2/ebook.html)“.

Complianceverstösse unterscheiden sich zudem von Land zu Land erheblich. Wo deutsche Unternehmen über ausländische Niederlassungen, Tochtergesellschaften, Zulieferer, Vertriebs- oder Handelspartner eingebunden sind, sind Kenntnisse der landesspezifischen Gesetzeslage zur Vermeidung von Haftungsrisiken unverzichtbar. Das „Handbuch Compliance international: Recht und Praxis der Korruptionsprävention (http://www.compliancedigital.de/ce/handbuch-compliance-international/ebook.html)“ gibt einen einzigartigen Überblick über die Grundlagen compliance-relevanter Rechtsgebiete bedeutender Wirtschaftsnationen

„Der ehrbare Kaufmann“

Nachricht vom 28.07.2015

Was ist ein ehrbarer Kaufmann und wie werde ich einer – bzw. was muss getan werden, damit es mehr „ehrbare Kaufmänner“ gibt? Antworten geben Christian Neßler und Bettina Lis in der aktuellen Ausgabe der ZCG.

Mythos oder Realität? Das Bild des ehrbaren Kaufmanns wird oft bemüht, um an das ethische Gewissen der heutigen Unternehmenslenker zu appellieren. Doch wer oder was ist ein ehrbarer Kaufmann und wie kann Staat und Unternehmen dafür Sorge tragen, dass sich Manager und Geschäftsführer „ehrbar“ verhalten?

Leitbild: „Der ehrbare Kaufmann“
Das Leitbild des ehrbaren Kaufmanns geht bis in das 12. Jahrhundert zurück – der Zeit der Hanse und des frühen Mittelalters in Italien. Ein Kaufmann galt damals als ehrbar, wenn er sein unternehmerisches Handeln an Tugenden wie Integrität, Aufrichtigkeit, Verlässlichkeit oder Anstand ausrichtete. Sein Wort hatte jederzeit Gültigkeit und sein Geschäftspartner konnte sich auf sein Wort verlassen. Verstieß er aber gegen diese Normen, musste er mit (gesellschaftlicher) Missbilligung rechnen.

Angesichts der Auswüchse der vergangen Jahre – meist ausgelöst von weniger ehrbaren Managern und Bankern – ist der Ruf lauter geworden, dass sich eben diese „Kaufleute“ wieder mehr an die alten Tugenden zurückbesinnen sollten. Das Stichwort heißt hier: Good Governance.

Good Governance – What is it good for?
Die Idee: Corporate-Governance-Kodizes – also die moralischen Grundregeln eines Unternehmens – sollen eine ordnungsgemäße Unternehmensführung im Grundsatz gewährleisten. Neben grundlegenden Regularien umfasst die Corporate Governance die spezifischen Grundsätze für eine gute und verantwortungsvolle Unternehmensführung und -überwachung. Die Corporate Governance soll, so die Idee dahinter, die gesetzlichen Spielregeln nicht abschaffen, sondern „vielmehr die Potenziale einer Unternehmenskultur, die am Verhalten der Mitarbeiter und deren Verantwortungsbewusstsein ansetzt“, herausstellen, so Neßler und Lis. Dies solle geschehen, „um das vorhandene Kotroll- und Regelinventar effektiver zu machen und eine Überregulierung zu vermeiden“.

Wie werde ich ein „ehrbarer Kaufmann“?
Doch was bringen all die Regularien am Ende? Neßler und Lis sagen nicht „Garnichts“. Aber – anstatt sich auf die Formulierung von Kodizes zu fokussieren, müsse verstärkt in der Ausbildung darauf geachtet werden, dass den Schülern und Studenten die Tugenden eines „ehrbaren Kaufmanns“ nahe gebracht werden. Letztlich, so die beiden Autoren, seien „Tugend und Integrität auch eine Frage der Erziehung und der persönlichen Einstellung.“ Ferner müssen Unternehmen bei der Ansprache und Rekrutierung der Mitarbeiter darauf achten, dass die potenziellen neuen Mitarbeiter in die „ehrbare“ Kultur des Unternehmens passen. Auch müssen die (potenziellen) Mitarbeiter bereit sein, die Tugenden zu bewahren und weiterzuentwickeln.

Den gesamten Beitrag von Dr. Christian Neßler und Dr. Bettina Lis „Good Governance – Mehr als nur eine Frage der Regulierung (http://www.compliancedigital.de/ce/good-governance-mehr-als-nur-eine-frage-der-regulierung/detail.html)“ können Sie in der aktuellen Ausgabe der ZCG (3/15) lesen.

Weitere Themen der aktuellen Ausgabe der ZCG

- „Stärkung der Qualität der Corporate Governance durch das geplante AReG? (http://www.compliancedigital.de/ce/staerkung-der-qualitaet-der-corporate-governance-durch-das-geplante-areg/detail.html)“ (Prof. Dr. Patrick Velte)
- „Unternehmensführung im Wandel: Von der Funktions- zur Prozessorientierung – Teil 1: Der Kraftakt eines organisationalen Musterwechsels (http://www.compliancedigital.de/ce/unternehmensfuehrung-im-wandel-von-der-funktions-zur-prozessorientierung/detail.html)“ (Prof. Dr. Markus H. Dahm, Aaron D. Brückner, Jörn B. Heyenrath)
- „Zur Bedeutung der Beziehungsqualität zwischen aktiven und passiven Gesellschaftern (eines Familienunternehmens) In der Praxis erfahrungsgemäß notwendige Gestaltungsmaßnahmen (http://www.compliancedigital.de/ce/zur-bedeutung-der-beziehungsqualitaet-zwischen-aktiven-und-passiven-gesellschaftern-eines-familienunternehmens/detail.html)“ (Susanne Simon-Baumann)
- „Public Corporate Governance Kodizes: Standardisierung durch einen Musterkodex? (http://www.compliancedigital.de/ce/public-corporate-governance-kodizes/detail.html)“ (Dr. Wilhelm Wilting)

Unternehmen merkeln in Sachen Datensicherheit

Nachricht vom 27.07.2015

Unternehmen tun nicht das, was sie tun müssten – nämlich ihre Sicherheitsvorkehrungen den aktuellen Cyberbedrohungen anzupassen, so eine aktuelle Studie der Wirtschaftsprüfungsgesellschaft EY.

Manche Dinge dürfte es eigentlich nicht mehr geben: Hütchenspieler, Kaffeefahrten oder aber auch der sorglose Umgang mit Unternehmensdaten. Doch immer noch fallen viele Menschen auf die alten Hütchenspieler-Tricks rein und täglich werden Unternehmen Opfer von Cyberangriffen und Datendiebstahl. In beiden Fällen – so scheint es – ist keine Besserung in Sicht.

Für den sorglosen Umgang mit dem Thema Datensicherheit in Unternehmen hat die Wirtschaftsprüfungsgesellschaft EY gerade neue Zahlen vorgelegt. Demnach nehmen zwar die Fälle von Cyberüberwachung und -kriminalität zu – das Risikobewusstsein deutscher Unternehmen dagegen nicht, so das Ergebnis der Studie „Datenklau: neue Herausforderungen für deutsche Unternehmen (http://www.ey.com/Publication/vwLUAssets/EY-Datenklau-2015-Praesentation-final/$FILE/EY-Datenklau-2015-Praesentation-final.pdf)“.

Unternehmensdaten sind leichte Beute
Laut der EY-Studie haben in den letzten drei Jahren 14 Prozent der deutschen Unternehmen konkrete Hinweise auf Spionageattacken entdeckt. Besonders betroffen sind vor allem große Unternehmen mit mehr als eine Milliarde Umsatz – hier ist sogar jedes fünfte Unternehmen betroffen. Doch nicht nur große Unternehmen und Behörden sind vom Datendiebstahl betroffen. Gerade kleinere und mittlere

Unternehmen (KMU) sind leichte Beute für Datendiebe. KMU haben häufig nicht die Mittel oder die Manpower, die notwendig wären, um die Netzwerke der Unternehmen so zu schützen, dass die sensiblen Produktions- oder auch Kundendaten vor illegalen Zugriffen sicher sind.

So ist es auch nicht verwunderlich, dass in jedem fünften Unternehmen (21 Prozent) die kriminellen Handlungen nur durch Zufall entdeckt wurden. Das, so eine andere Studie von den Unternehmensberatern von A.T. Kearney, ist allerdings auch nicht verwunderlich. In der Regel dauere es 243 Tage, bis ein Angriff entdeckt wird, so der IT-Sicherheitsexperte Dr. Boris Piwinger von A.T. Kearney (http://www.compliancedigital.de/ce/cyber-attacken-sind-genauso-wenig-vorhersagbar-wie-erdbeben/detail.html).

(K)ein Grund zur Sorge

Viele Unternehmen merkeln – um einen Topfavoriten auf das Jugendwort des Jahres 2015 zu zitieren – in Sachen Datensicherheit. Die „anhaltende Sorglosigkeit" – oder das Aussitzen im Merkelschen Sinne – überrasche, so Bodo Meseke, Leiter Forensic Technology & Discovery Services bei EY. Viele Unternehmen denken, „sie seien ausreichend geschützt oder würden nicht Ziel von Datenklau und Cyberangriffen werden. Dabei zeigen die immer neuen Enthüllungen, dass jeder Ziel solcher Attacken werden kann und dass die gängigen Schutzmechanismen umgangen werden können."

Unternehmen setzen auf einfache Schutzmaßnahmen

Die anhaltende Sorglosigkeit spiegelt sich auch in den Schutzmaßnahmen wider. 82 Prozent der befragten Manager halten die getroffenen präventiven Maßnahmen gegen Datendiebstahl für ausreichend, wie Firewalls, Antivirensoftware und gute Passwörter – immerhin!

Umfassende Schutzmaßnahmen sucht man dagegen vergeblich. Ein Intrusion-Detection- bzw. Prevention-System, das Hinweise auf die Aktivitäten von Eindringlingen in das eigene Netzwerk geben kann, haben lediglich nur 30 Prozent der Unternehmen. Das ist immerhin eine Steigerung von 100 Prozent im Vergleich zu 2013.

Dieses Verhalten sei schlicht und ergreifend „fahrlässig", so Meseke. „Passwörter und Antivirensoftware können von Hackern heute mitunter minutenschnell umgangen werden. Ein Sicherheitssystem, das lediglich auf diese herkömmlichen Schutzmaßnahmen setzt, öffnet Hackern bereitwillig die Tore. Wer sensible Firmen- oder Kundendaten auf seinen Servern hat, sollte unbedingt strengere Sicherheitsvorkehrungen einführen", so Meseke.

Literaturempfehlung zum Thema IT-Sicherheit

Seit Anfang Juli steht die Zeitschrift Privacy in Germany (PinG) Abonnenten von COMPLIANCEdigital kostenfrei zur Verfügung. Die Zeitschrift setzt sich Schwerpunktmäßig auf mit Fragen der Daten- und IT-Sicherheit auseinander (http://www.compliancedigital.de/short/ping/ejournal-inhalt.html).

Eine praxis2orientierte Einführung in die Welt der IT-Prüfung bietet Stefan Beißel in dem Band „IT-Audit: Grundlagen – Prüfungsprozess – Best Practice (http://www.compliancedigital.de/ce/it-audit/ebook.html)". Anhand eines umfassenden Prüfungskatalogs können Sie systematisch erschließen, worauf es bei der Vorbereitung, der Durchführung und dem Abschluss erfolgreicher IT-Audits ankommt.

Wie Unternehmen wesentliche regulatorische Anforderungen an die IT identifizieren, priorisieren und effizient steuern können, erläutern die Autoren Michael Rath und Rainer Sponholz in dem Band „IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen (http://www.compliancedigital.de/ce/it-compliance-7/ebook.html)".

Ausscheidende Mitarbeiter

Nachricht vom 21.07.2015

Die wichtigste Ressource sind die Mitarbeiter – auch für die Compliance. Auch diejenigen, die gehen, sind als Quelle wichtig, so Thomas Schneider, Autor des Bandes „Mitarbeiter-Compliance".

Im Teil 4 der Serie zum Thema „Mitarbeiter-Compliance" hat Thomas Schneider die Frage beantwortet, wann der beste Zeitpunkt wäre, Mitarbeiter, die neu in das Unternehmen kommen, mit den Compliance-Regeln des Hauses vertraut zu machen (http://www.compliancedigital.de/ce/einstieg-ins-unternehmen-1/detail.html). Im Teil 5 richtet der Autor des Bandes „Mitarbeiter-Compliance (http://www.compliancedigital.de/ce/mitarbeiter-compliance/ebook.html)„ nun den Blick auf die Mitarbeiter, die das Unternehmen verlassen (müssen).

Den richtigen Gesprächs-Zeitpunkt finden

Genauso wichtig, wie der Einstieg, ist aus Sicht der Compliance auch der Ausstieg eines Mitarbeiters. Dementsprechend sollte der Compliance-Officer rechtzeitig das Gespräch mit dem Mitarbeiter suchen, der das Unternehmen verlässt. Das Gespräch sollte nicht in der Hektik der letzten Arbeitswoche stattfinden, sondern idealerweise etwa einen Monat vor dem Ausscheiden.

Da sich Compliance-Officer und der ausscheidende Mitarbeiter idealerweise bereits kennen, kann der Gesprächsgrund offen angegeben werden – was für den weiteren Gesprächsverlauf förderlich ist: Die Compliance möchte letzte Informationen gewinnen, aber auch ein offenes Feedback für die eigene Tätigkeit erhalten. Taktische Aussagen von Seiten der Mitarbeiter sind auch nicht mehr notwendig, da der Mitarbeiter in der Regel keine Rücksicht mehr nehmen muss.

Aber Vorsicht: Eine absolute Wahrheit kann es nie geben! Der Informationsgehalt der Aussagen ist dennoch ein anderer als bei Gesprächen, in denen immer bewusst ist, dass auch die Compliance über Sanktionsmöglichkeiten verfügt. Wichtig – und das muss auch zugesichert werden: Das Gespräch bleibt vertraulich und der ehemalige Vorgesetzte des Mitarbeiters darf nicht über den Verlauf informiert werden.

Ausstiegs-Gespräch: Worum geht es?

An erste Stelle geht es darum, an den Erfahrungen des Gesprächspartners teilzuhaben. Dabei steht die Compliance im Mittelpunkt. Wie wurden die Vorgaben im Arbeitsalltag erlebt? Wo wurde die Tätigkeit erleichtert, wo erschwert? Welche Veränderungen wurden im Zeitablauf erfahren? Explizit sollte Verbesserungspotential angesprochen werden. Dabei hat der Gesprächsverlauf bewusst allgemeinen Charakter.

Auch der Compliance-Officer sollte ein eigenes Feedback einbringen. Wie hat der Mitarbeiter auf ihn gewirkt? Wo war eine kooperative Zusammenarbeit möglich? Wo gab es Hindernisse, Misstrauen, ja Widerstände? Zwar mag der Mitarbei-

ter nicht mehr vom Feedback beruflich profitieren, allerdings kann dieser seine Motive erläutern, damit der Compliance-Mitarbeiter diese nachvollziehen kann. Dabei sollte auch das eigene Austreten thematisiert werden. Zwar kann es ein Compliance-Officer nicht allen rechtmachen. Wo aber Differenzen die fachliche Dimension überschritten haben, besteht Erklärungs- und Handlungsbedarf.

Sicherlich besteht seitens der Compliance auch Interesse an möglicherweise kritischen Vorgängen aus der Vergangenheit, die bisher weder angegeben, noch aufgedeckt wurden. Auf dieses Thema zu drängen, wird selten erfolgreich sein. Eher sollte eine langsame Über-leitung erfolgen, die das Nachfragen nach Schwachstellen der Internen Revision als auch der Compliance bei einzelnen Prüfungen in den Mittelpunkt stellt.

Hier große Erwartungen zu hegen, führt aber eher zu Enttäuschungen. Trotzdem sollten die Hinweise ernst genommen werden. Ergeht sich der Gesprächspartner in Andeutungen, kann durchaus offensiv reagiert werden, wenn diese für konkrete Schritte nicht ausreichen.

Ohne weitere Informationen sind der Compliance aber die Hände gebunden. Auf nebulöse Vorwürfe und Verdächtigungen sollte der Compliance-Officer allerdings nicht eingehen. Möchte der Mitarbeiter nicht konkreter werden, wird auf die Möglichkeit verwiesen, auch nach Ausscheiden aus dem Unternehmen den Kontakt nicht abreißen zu lassen. Der Fairness halber gilt es, darauf hinzuweisen, dass auch Ehemalige nach dem Ausscheiden zivil- und strafrechtlich haftbar gemacht werden können.

Serie Mitarbeiter-Compliance
Teil 1: „Compliance: Ein Thema aller Mitarbeiter (http://www.compliancedigital.de/ce/compliance-ein-thema-aller-mitarbeiter/detail.html)“
Teil 2: „Was Compliance-Verantwortliche von Geheimdiensten lernen können (http://www.compliancedigital.de/ce/was-compliance-verantwortliche-von-geheimdiensten-lernen-koennen/detail.html)“
Teil 3: „Die Welt vor Compliance (http://www.compliancedigital.de/ce/die-welt-vor-compliance/detail.html)“
Teil 4: „Einstieg ins Unternehmen (http://www.compliancedigital.de/ce/einstieg-ins-unternehmen-1/detail.html“

Weitere Informationen zu dem Thema gibt das Buch „Mitarbeiter Compliance (http://www.compliancedigital.de/ce/mitarbeiter-compliance/ebook.html)“, welches im Erich Schmidt Verlag erschienen ist.

Killt Compliance die Kunst?

Nachricht vom 17.07.2015

Sommerzeit ist Festspielzeit. Doch nicht nur Künstler sondern auch Kulturmanager haben Hochsaison, müssen sie doch die Sponsoren bei Laune halten.

Ohne Sponsoring sind die meistens Events, wie die Salzburger- oder Bregenzer Festspiele undenkbar. Egal ob Autofirmen wie Audi, BMW, Mercedes oder Banken und Fluglinien – alle wollen mit Hilfe von Sponsoring ihre Marke näher an die zahlungskräftige Kundschaft bringen.

„Überzogene Compliance-Richtlinien machen der Kunst zu schaffen“
Ob Einladungen in die „Vip-Lounge“ oder exklusive Sitzplätze – Unternehmen lassen sich nicht lumpen. Doch die goldenen Zeiten der Firmeneinladungen sind vorbei, so die langjährige Präsidentin der Salzburger Festspiele, Helga Rabl-Stadler, gegenüber dem Handelsblatt.

Der Grund: Viele Unternehmen haben in der Vergangenheit „Kultur als Schmiermittel“ benutzt, so dass der Gesetzgeber reagieren musste. Erst im vergangenen Jahr hat Deutschland nach langem Zögern das Übereinkommen der Vereinten Nationen (UNO) gegen Korruption ratifiziert, Österreich bereits im Jahr 2006. In den Augen von Rabl-Stadler schlage das Pendel aber zu sehr aus.

„Die überzogenen Compliance-Richtlinien machen uns zu schaffen. Sowohl der Einladende und der Geladene schrecken zurück. Das schadet allen Kultur- und Sportveranstaltern“. Nach ihrer Meinung sei die „ganz normale Gastfreundschaft in Verruf geraten. Ein Tribut an die Neidgenossenschaft. Das ist ein Problem der heutigen Zeit.“

Politik in der Compliance-Falle?
Laut Rabl-Stadler habe die Politik das Problem erkannt. „Alle Politiker sagen im Vier-Augen-Gespräch, wir wissen, dass die Compliance-Regeln übertrieben sind.“ Allerdings könnten die Politiker dagegen „nichts machen“, so die Präsidenten der Salzburger Festspiele. In dem Interview kritisierte Rabl-Stadler zudem, dass zwar Spenden an soziale Institutionen absetzbar seien, an die Kunst jedoch nicht. „Das ist ein Fehler“, so die Festspiel-Präsidentin.

Leitfaden zum Umgang mit Sponsoring
Bereits im vergangenen Jahr haben das Deutsche Global Compact Netzwerk (DGCN) und das Deutsche Institut für Compliance (DICO) den Leitfaden zur Korruptionsbekämpfung (http://www.compliancedigital.de/ce/praxisleitfaden-korruptionsbekaempfung/detail.html) aufgelegt. Ein zentrales Thema: Sponsoring. Welche konkreten Compliance-Risiken auf die Unternehmen lauern, beschreibt Sylvia Schenk von Transparency International Deutschland e.V. (http://www.globalcompact.de/sites/default/files/themen/publikation/korruptionspraevention._ein_leitfaden_fuer_unternehmen.pdf) (Quelle: Handelsblatt)

Literaturempfehlung Compliance und Sponsoring
Das „Handbuch Compliance international (http://www.compliancedigital.de/ce/handbuch-compliance-international/ebook.html)“, herausgegeben von Dr. Malte Passarge und Prof. Dr. Stefan Behringer, beleuchtet neben den Grundlagen compliance-relevanter Rechtsgebiete auch das Thema Sponsoring und Korruption. Compliance-Experten gehen besonders auf die Korruptionsbekämpfung in folgenden Ländern ein: Australien, Belgien, China, Deutschland, Frankreich, Großbritannien, Indien, Italien, Japan, Osttimor, Österreich, Polen, Russland, Schweiz, Südafrika, Südkorea, Tschechien, Türkei, USA.
Auf die besonderen Herausforderung im Vertrieb gehen Wolfgang Schärpf und Hiltrud Walz in dem ZIR-Beitrag „Prüfung der Compliance von vertrieblichen Kooperationen: Ein Orientierungsrahmen für Revisoren (http://www.compliancedigital.de/ce/pruefung-der-compliance-von-vertrieblichen-kooperationen/detail.html)“ ein.

Dienstreisen waren gestern

Nachricht vom 17.07.2015

Wie sieht ein modernes Travel Management aus? Der neue Prüfungsleitfaden vom DIIR Arbeits-

kreis „Revision Personalmanagement und interne Dienstleistungen" gibt hierüber Auskunft.

Die Zeiten, als es in Sachen Dienstreisen lediglich um die Überprüfung der Reiseabrechnung ging, sind lange vorbei. Geschäftsreisen sind heute komplexe Vorgänge – und daher auch für die Interne Revision ein wichtiges Betätigungsfeld. Ein lang vernachlässigtes Thema ist dabei das Thema Sicherheit. Viele Geschäftsreisende fühlen sich in Sicherheitsfragen unzureichend von Ihren Unternehmen informiert (http://www.compliancedigital.de/ce/vermeidbare-sicherheitsrisiken-auf-geschaeftsreisen/detail.html). Um der gewachsenen Bedeutung Rechnung zu tragen, sprechen Interne Revisoren daher auch von Travel Management.

Travel Management bedeutet eine umfassendere Aufgabenstellung

„Travel Management" beschreibt in Anlehnung an den Verband Deutsches Reisemanagement die strategischen und operativen Maßnahmen zur Planung, Organisation und Kontrolle der Geschäftsreiseaktivitäten des Unternehmens (beziehungsweise einer Einrichtung im öffentlichen Sektor).

Das Travel Management umfasst dabei folgende Aufgaben:

- Schaffung der Strukturen für die Planung und Abwicklung von Geschäftsreisen und die Gestaltung effizienter Prozesse
- Förderung des effektiven Einsatzes von Geschäftsreisen
- Ermöglichung einer effizienten, ressourcenschonenden und sicheren Umsetzung
- Sicherstellung der ordnungsgemäßen Abwicklung der Geschäftsreisen gemäß den rechtlichen Rahmenbedingungen und den Unternehmensspielregeln
- Berücksichtigung des „Motivationsfaktors" der Geschäftsreise-Regularien (z. B. Zeit, Komfort, Sicherheit)

Der vom DIIR-Arbeitskreis „Revision Personalmanagement und interne Dienstleistungen" entwickelte Leitfaden beschreibt typische Prüfungsansätze, um die Wirksamkeit von Travel-Management-Systemen zu beurteilen und zu verbessern.

Den Prüfungsleitfaden „Travel Management: Revision von Geschäftsreisen", der soeben in dritter Auflage erschienen ist, können Sie hier (http://www.esv.info/978-3-503-15872-0) bestellen.

Ist mein Geschäftspartner compliant?

Nachricht vom 14.07.2015

Steigende regulatorische Anforderungen führen zu mehr Investitionen in die Compliance. Verstärkt rücken zudem die Geschäftspartner in den Fokus, wie eine aktuelle Umfrage zeigt.

Deutsche Unternehmen investieren verstärkt in ihre Compliance Management Systeme (CMS), so das Ergebnis der aktuellen Umfrage „Die Praxis der Geschäftspartner-Compliance in deutschen Unternehmen – Ergebnisse (http://www.berlinrisk.de/Media/Downloads/BR_8_25_Studie_Gesch%C3%A4ftspartner_Compliance_2015.pdf)" von LexisNexis und Berlin Risk.

Danach beschäftigen sich 29 Prozent der Unternehmen mit dem Aufbau einer Compliance-Organisation. 90 Prozent sind mit der Aktualisierung und Weiterentwicklung des CMS beschäftigt und wiederum 38 Prozent der befragten Unternehmen waren darüber hinaus mit Schulungen befasst.

Aktualisierung und Weiterentwicklung des CMS

Doch welche Maßnahmen werden konkret von den Unternehmen in Bezug auf die CMS angegangen? Laut der Umfrage stehen folgende Punkte auf der To-do Liste:

- Durchführung einer Compliance-Risikoanalyse und ein regelmäßiges Risikomonitoring
- Umfassende Risikoanalyse und regelmäßige Überprüfung
- Einführung eines konzernweiten weltweiten Code of Conduct
- Klauseln in Verträgen
- Beobachtung der Gesetzesentwicklung/Rechtsprechung
- Ausrichtung des CMS an neuen Anforderungen / Anpassung von Regelwerken/Erweiterung der Themenfelder
- Weiterentwicklung der Systeme und Tools
- Kontinuierliche Anpassung der Geschäftspartner-Compliance an die geänderten Bedingungen
- Intranet mit Richtlinien, Verhaltensregeln und Möglichkeiten der Kommunikation für Hinweisgeber
- Entwicklung von Fragebögen
- Durchführung von Audits
- Erhöhung des Budgets und die Ernennung von zusätzlichen Compliance-Beauftragten
- Bestellung von mindestens einem verantwortlichen Compliance Officer (CO) in jedem Land – Compliance wird als Management-Aufgabe gesehen. Die CO in einzelnen Ländern haben andere operative Hauptaufgaben und sollen das lokale Management bei der Umsetzung der Compliance-Strukturen unterstützen, aber auch mahnen, wenn notwendig
- Jährliche Berichterstattung im Prüfungsausschuss des Konzern-Aufsichtsrates

Geschäftspartner als Compliance-Herausforderung

Als Herausforderungen sehen die befragten Unternehmen vor allem die Themen

- Geschäftspartnerprüfung,
- die vierte Geldwäsche-Richtlinie der EU sowie
- andere Elemente der Prävention von Wirtschaftskriminalität.

Vor allem das Thema Geschäftspartnerprüfung treibe die Unternehmen um, so das Ergebnis der Umfrage. Bereits auf dem diesjährigen LexisNexis Compliance Solution Day stand das Thema Geschäftspartner-Compliance ganz oben auf der Agenda (http://www.compliancedigital.de/ce/den-geschaeftspartner-im-auge-behalten/detail.html).

Den Grund für die verstärkte Aufmerksamkeit auf die Geschäftspartner formulierte der Tagungsleiter Prof. Fetzer: „Sag mir, wer deine Freunde sind und ich sage Dir, wer Du bist". Auf die internationale Geschäftswelt umgemünzt bedeutet dies, dass Verfehlungen eines Geschäftspartners sehr schnell zu eigenen werden können – ob man wolle oder nicht.

Sorge bereite den Unternehmen in Bezug auf deren Geschäftspartner vor allem

die Themen Arbeitsstandards und Menschenrechte.

Wie kann man seinen Geschäftspartner prüfen?
Zur Überprüfung der Geschäftspartner setzen die meisten Unternehmen auf Datenbank-Recherchen. Am Ende der Maßnahmen steht dagegen der Vorort-Besuch. Diese Prüfpunkte sind sinnvoll:
1. Datenbank-Recherchen
2. Fragebogen
3. Internet-Recherchen
4. Einsatz externer Dienstleister
5. Risk Assessment
6. Integrierte Softwarelösung
7. Referenzen / Persönliches Gespräch
8. Audit / Monitoring
9. Vorort-Besuche

Literaturempfehlungen für Geschäftspartner-Compliance
Eine Herausforderung für jede internationale Unternehmung sind trotz weltweiter Harmonisierungsbemühungen die unterschiedlichen Rechtslagen und die Rechtspraxis bei Compliance-Verstößen. Das „Handbuch Compliance International (http://www.compliancedigital.de/ce/handbuch-compliance-international/ebook.html)“ gibt einen einzigartigen Überblick über die Grundlagen compliance-relevanter Rechtsgebiete bedeutender Wirtschaftsnationen.
Der Band „Risikomanagement in Supply Chains (http://www.compliancedigital.de/ce/risikomanagement-in-supply-chains-1/ebook.html)“, herausgegeben von Prof. Dr. Christoph Siepermann Prof. Dr. Richard Vahrenkamp und Dr. Markus Siepermann gibt einen systematischen Überblick über die in Supply Chains auftretenden Risiken. Die Autoren zeigen zugleich Strategien zum Umgang mit den Risiken auf.

Cyberrisiken nehmen zu – die Abwehr aber auch

Nachricht vom 10.07.2015

Cyberrisiken werden immer mehr zur Bedrohung der gesamten Wirtschaft. Sicherheitsbehörden und Aufsichtsbehörden reagieren auf das Bedrohungsszenario – zu spät oder noch rechtzeitig?

Cyberrisiken sind längst nicht mehr zu Leugnen. Fast täglich erreichen uns Nachrichten über gehackte Netzwerke, geklaute Daten und gekaperte Webseiten. Jüngster Fall: Wie die FAZ berichtet, sollen Hacker aus China bei der US-Bundesverwaltung Daten von rund 21,5 Millionen Menschen entwendet haben. Die Hacker hatten demnach Zugriff zu Adressen, Sozialversicherungsnummern, Geburts- und Gesundheitsdaten sowie Informationen zu Finanzen, krimineller Vergangenheit und auch Fingerabdrücken der Betroffenen.

Leichtes Spiel für Hacker
Auch deutsche Firmen und Behörden stehen im Visier. Immer noch unklar ist etwa, woher die Hacker kamen, die in das IT-Netzwerk des deutschen Bundestages eingedrungen sind.

Laut der aktuellen Bitkom-Studie zu „Wirtschaftsschutz und Cybercrime“ waren 51 Prozent aller Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage. Der Schaden belaufe sich nach Schätzungen von Bitkom auf rund 51 Milliarden Euro pro Jahr. Besonders betroffen sind laut der Studie vor allem die Automobilindustrie, die Chemie- und Pharmabranche sowie Banken und Versicherungen.

Trotz dieser Bedrohung schützen Unternehmen ihre IT-Infrastruktur allerdings nur unzureichend. Laut der aktuellen A.T. Kearney-Studie „Information Security: It's All About Trust (http://www.compliancedigital.de/ce/cyber-attacken-sind-genauso-wenig-vorhersagbar-wie-erdbeben/detail.html)“ agieren viele Unternehmen immer noch zu langsam, um mit der rasanten Entwicklung der Angriffe Schritt zu halten. Im Schnitt dauere es 243 Tage, bis ein Cyber-Angriff entdeckt wird. In dieser Zeit haben Hacker genügend Zeit, sich „nach interessanten Daten umzusehen und das gesamte Unternehmen flächendeckend zu infiltrieren“, so der Studienautor und Leiter des Beratungsbereichs Informationssicherheit bei A.T. Kearney, Dr. Boris Piwinger.

Hufeld: Cyberrisiken im Finanzsektor haben ein alarmierendes Niveau erreicht“
Auf dem Bundesbank Symposium „Bankenaufsicht im Dialog“ in Frankfurt am Main warnte Felix Hufeld, Präsident der BaFin, ebenfalls vor der zunehmenden Gefahr aus dem Netz: Die „Qualität der Cyberrisiken im Finanzsektor“ habe nach Ansicht von Hufeld „ein alarmierendes Niveau erreicht“.

Hierauf müssen sowohl die Banken als auch die Aufsichtsbehörden reagieren. Die Herausforderung bestehe darin, dass auch die Aufsichtsbehörden sich gerade in einer gewaltigen Lernkurve befinden. Denn, so viel ist sicher, das Thema Cyber-Security ist nur im Zusammenspiel von aufsichtlichem, technischem und kriminalistischem Know-how zu bewältigen.

Folgende Maßnahmen wurden auf Seiten der Aufsichtsbehörden bereits in Angriff genommen:
- Bei der Europäischen Bankenaufsichtsbehörde (EBA) wurde eine Task-Force zu IT-Risiken gegründet, die neue Anforderungen an die IT-Organisation der Banken in Europa aufstellen wird. Sie bildet die Basis für eine einheitliche IT-Aufsicht.
- Die BaFin hat in Zusammenarbeit mit der Bundesbank Prüfungsmodule zu IT-Prüfungen erarbeitet. Diese werden bei den Arbeiten der EBA als auch in den Single Supervisory Mechanism (SSM) eingebracht.
- Die EZB untersucht gerade die Widerstandsfähigkeit der bedeutenden Banken gegen Cyber-Attacken (sog. Cyber-resilience). Nach Auswertung der Erhebungen werden konkrete Maßnahmen beschlossen.

Maaßen: Cyber-Security ist zu einer „vorrangigen Aufgabe der Sicherheitsbehörden geworden“
Neben den Aufsichtsbehörden müssen auch die Sicherheitsbehörden auf die neue Bedrohungslage reagieren. Der Schutz hochsensibler Informationen und kritischer Infrastrukturen ist nach Auffassung von Dr. Hans Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz „zu einer vorrangigen Aufgabe der Sicherheitsbehörden geworden“. Es bedarf daher, so Maaßen in seinem Beitrag „Cyberwar – eine reale Gefahr aus der virtuellen Welt (http://www.compliancedigital.de/ce/cyberwar-eine-reale-gefahr-aus-der-virtuellen-welt/detail.html)“ für die neue Fachzeitschrift auf COMPLIANCEdigital, PinG, einer „umfassenden, gesamtgesellschaftlichen Strategie“, um Cyberwar, -Spionage und Infokrieg entgegenzuwirken. Abwehrmöglichkeiten müssten optimiert werden – technisch, rechtlich und analytisch.

Maaßen: IT-Sicherheitsgesetz ist ein „Meilenstein"

Integraler Bestandteil der Maßnahmen ist das gerade verabschiedete IT-Sicherheitsgesetz. Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist in den Augen von Maaßen ein „Meilenstein". Auch die BaFin begrüßt die gesetzgeberische Initiative: Die BaFin werde das Bundesamt für Sicherheit in der Informationstechnik bei der weiteren Ausgestaltung des Gesetzes bzw. der danach zu erlassenden Verordnung unterstützen. Klar muss aber auch sein, dass die neuen Möglichkeiten nicht zu einer blinden Sammelwut bei Sicherheitsbehörden führen", so Maaßen (siehe hierzu auch der Beitrag auch COMPLIANCEdigital vom 20.04.2015 (http://www.complIancedigital.de/ce/freie-fahrt-fuer-staatliche-datensammler/detail.html)). (Quelle: Bitkom, A.T.Kearney, BaFin)

Literaturempfehlung zum Thema IT-Sicherheit

Seit Anfang Juli steht die Zeitschrift Privacy in Germany (PinG) (http://www.complIancedigital.de/ce/ping-neu-auf-complIancedigital/detail.html) Abonnenten von COMPLIANCEdigital kostenfrei zur Verfügung. In der aktuellen Ausgabe (4/2015) gehen die Autoren der Frage nach, wie die richtige Balance zwischen Freiheit und Sicherheit in einem Rechtstaat gefunden werden kann?

Wie Unternehmen wesentliche regulatorische Anforderungen an die IT identifizieren, priorisieren und deren Erfüllung einer effizienten Steuerung zuführen, erläutern Michael Rath und Rainer Sponholz in dem Band „IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen (http://www.complIancedigital.de/ce/it-compliance-7/ebook.html)".

Eine praxisorientierte Einführung in die Welt der IT-Prüfung bietet Stefan Beißel in dem Band „IT-Audit: Grundlagen – Prüfungsprozess – Best Practice (http://www.complIancedigital.de/ce/it-audit/ebook.html)". Anhand eines umfassenden Prüfungskatalogs können Sie systematisch erschließen, worauf es bei der Vorbereitung, der Durchführung und dem Abschluss erfolgreicher IT-Audits ankommt.

Risk Assessment als integraler Bestandteil eines CMS

Nachricht vom 09.07.2015

Welche Aspekte müssen bei der Durchführung eines Risk Assessement in der Pharmabranche beachtet werden? Der Leitfaden von Christian Weimar und Willibert Franzen gibt einen Überblick.

Die Pharmabranche steht schon seit längerem im Fokus der Ermittlungsbehörden – vor allem in den USA (http://www.complIancedigital.de/ce/fcpa-und-die-pharmabranche-eine-stellungnahme-der-sec/detail.html). Grund hierfür sind nicht zuletzt die vielen Korruptionsskandale der Vergangenheit, die den Ruf der Branche nicht gerade gefördert haben. Der neueste Fall: Novartis. Trotz intensiver Compliance-Maßnahmen (http://www.complIancedigital.de/ce/compliance-zu-den-mit-arbeitern-bringen-aber-wie/detail.html) wurde letzte Woche bekannt, dass dem Schweizer Pharmakonzern eine Milliardenstrafe in den USA droht. Laut Information des Handelsblatts soll Novartis sich illegaler Vertriebspraktiken beim Medikamentenverkauf bedient haben. Novartis bestreitet die Vorwürfe und will sich vor Gericht gegen die Vorwürfe wehren.

Pharmabranche muss Compliant werden

Ganz gleich, wie der aktuelle Prozess ausgeht: Compliance umfasst auch in der Pharmaindustrie nicht länger nur die Kooperationsbereitschaft eines Patienten während einer Therapie, sondern auch der Umgang mit Gesetzesverstößen.

Die meisten Pharmafirmen – auch in Deutschland – haben in den vergangen Jahren umfangreiche Compliance Management Systeme (CMS) aufgebaut. Integraler Bestandteil eines CMS muss dabei, so die Meinung von Christian Weimar und Dr. Willibert Franzen, ein Compliance Risk Assessment (CRA) sein, auch wenn es nach deutscher Gesetzeslage hierfür keine explizite gesetzliche Pflicht gebe.

CRA nicht zwingend, aber dennoch erforderlich

Indirekt ergebe sich allerdings aus den §§ 30, 130 OwiG die Pflicht zur geeigneten Überwachung der Risiken. Aus den § 43 GmbHG bzw. § 93 AktG leitet sich darüber hinaus auf die Legalitätspflicht ab. Agieren die Pharmafirmen international, leitet sich die systematische Risikoinventur aus dem UK Bribery Act oder dem Foreign Corrupt Practices Act (FCPA) ab. Auch im IDW PS 980 wird unter Tz. A16 das Vorhalten eines CRA eingefordert.

Wie wird die Pharmabranche Compliant?

Ob mit oder ohne Gesetzesvorgabe. Nur ein Risk Assessment biete die Möglichkeit, flächendeckend unternehmensweite Compliance Risiken zu identifizieren und zu evaluieren, so die Auffassung der Autoren. Die Durchführung eines CRA ist selbst mit hohen Risiken behaftet. Was muss bei der Durchführung beachtet werden:

- Commitment der Unternehmensleitung: Der Erfolg eines CRA steht und fällt mit dem Commitment der Geschäftsführung. Steht diese nicht geschlossen hinter der Maßnahme, sind die Erfolgsaussichten schlecht.
- Festlegung des Erhebungsumfangs: Um das CRA zielorientiert und kosteneffizient durchführen zu können, ist die Determination des Erhebungsumfangs wichtig. Findet die Maßnahme zum ersten Mal statt, empfiehlt es sich, mit den Verantwortlichen sämtlicher Bereiche vorab zu sprechen, um abschätzen zu können, wo die meisten Risiken auftreten können
- Compliance Risk Matrix: Um die Komplexität des CRA in Griff zu behalten, empfehlen die beiden Autoren die Verwendung der Compliance Risk Matrix, die – im Nachgang – mit Excel weiter fortgeführt und gepflegt werden kann.
- Mitarbeiterbefragung: Top-down vs. Bottom-up. Ein CRA kann darüber hinaus nur erfolgreich durchgeführt werden, wenn die Mitglieder des Unternehmens persönlich befragt bzw. interviewt werden. Grundlegend und daher selbstredend muss die Befragung der Mitarbeiter bzw. der Führungskräfte gründlich vorbereitet werden. Nur dann, so die Autoren, liefere die Befragung tatsächlich neues, relevantes Wissen.

Den gesamten Beitrag von Christian Weimar und Dr. Willibert Franzen mit weiteren Hintergrundinformationen lesen Sie in der aktuellen Ausgabe der ZCG 3/2015 (http://www.complIancedigital.de/ce/compliance-risk-assessment-konzepte-und-ein-praxisorientierter-leitfaden/detail.html) . (Quelle: ZCG, Handelsblatt)

Literaturhinweis Pharmaindustrie

In Kürze erscheint das von Prof. Joachim S. Tanski herausgegebene Standardwerk „Interne Revision im Krankenhaus (http://www.esv.info/978-3-503-16303-8)"

in der zweiten Auflage. Den Band können Sie hier bereits vorbestellen.
Die Zeitschrift Krankenhaus-Rechtsprechung (KRS) informiert Sie jeden Monat über die wichtigsten Entscheidungen zum gesamten Krankenhausrecht. Fordern Sie hier (http://www.esv.info/add/ZPA.KRS/_sid/FJCO-108101-TrTx/warenkorb.html) gleich ihr Testabonnement an!

Den Geschäftspartner im Auge behalten

Nachricht vom 07.07.2015

Screenings und Due Diligence Investigations sind für internationale Geschäftskontakte unabdingbar. Wo liegen die Vorteile und wie können Compliance Officer profitieren?

In Zeiten von Sanktions- und Embargo-Listen steht immer öfter die Frage im Raum wer eigentlich der Geschäftspartner ist: Handelt es sich wirklich um die verantwortliche Person oder ist die Person lediglich ein sogenannter Strohmann? Die Überprüfung von Geschäftspartnern gehört gerade für Unternehmen – die Geschäfte mit unsicheren Ländern betreiben – überlebenswichtig, so Dr. Roman Zagrosek, Geschäftsführer der Compliance Solutions GmbH auf dem diesjährigen LexisNexis Compliance Solutions Day in München (http://www.compliancedigital.de/ce/geschaeftsherrenmodell-und-iso-19600-fuer-die-compliance/detail.html).
Compliance Officer sind darauf angewiesen – um eine effiziente und rechtssichere Geschäftspartnerüberprüfung sicherzustellen – ausreichende Informationen zur Verfügung zu haben. Geschäftspartner Screening und Due Diligence Investigation (DDI) sind zwei Instrumente, an diese zu gelangen.

Geschäftspartner Screening

Grundlegend gilt, dass Unternehmen auch für Ihre Geschäftspartner verantwortlich sind.

„Wilfull blindness exkulpiert nicht", so Zagrosek in seinem Vortrag (http://www.lexisnexis.de/events/compliance-day-2015/geschaeftspartnerueberpruefung-compliance-solutions.pdf). Die Risiken für Unternehmen reichen von

- Sanktionen und Vorteilsabschöpfung, über
- Schadensersatz und
- Steuer- und Bilanzrechtsprobleme
- Vergaberechtliche Konsequenzen, bis hin zu
- Reputationsschäden.

Gerade letzteres ist für die Unternehmen immer wichtiger, wie Tagungsleiter Prof. Fetzer hervorhob: „Sag mir, wer deine Freunde sind und ich sage Dir, wer Du bist". Auf die internationale Geschäftswelt umgemünzt bedeutet diese Volksweisheit, dass Verfehlungen meines Geschäftspartners sehr schnell zu meinen werden können – ob man wolle oder nicht.

Verfolgungsbehörden verlangen daher von den Unternehmen ein umfangreiches Geschäftspartner-Screening. Dies beinhaltet vor allem, dass alle zugänglichen Informationen, wie Sanktions-, PEP- und Blacklisten berücksichtigt werden. Die Recherche umfasst automatisierte Checks, Compliance Web Recherche, externe Recherchen sowie sogenannte Third Party KYC Solutions, wie z. B. bereitgestellt von LexisNexis und info4c.

Recherche ist gut, Due Diligence Investigation ist besser

Doch was passiert, wenn die Quellen nicht alle Informationen Preis geben, die benötigt werden? Oftmals sehe die Realität anders aus als auf dem Papier. Hier bedürfe es des Blicks hinter die Kulissen, um eine qualifizierte Risikoanalyse vornehmen zu können. Aus Compliance-Sicht stellt sich zudem die Frage, wie weit über die definierte Compliance hinaus recherchiert und dokumentiert werden muss, um für einen eventuellen Streitfall gewappnet zu sein?

Informationen, wie

- dem politischen System (Gesetzeslage, Regierung, Parteien),
- den Gewerkschaften und
- den Ansprechpartnern vor Ort

können noch im Rahmen eines Target Business Assessment beantwortet werden.

Schwieriger wird es aber, wenn Hintergrundinformationen zu den Geschäftspartnern und der Situation vor Ort benötigt werden:

- Handelt es sich tatsächlich um den Geschäftspartner, der offiziell benannt wurde?
- Welche Historie hat der Geschäftspartner und wie ist seine Reputation?
- Ist der Geschäftspartner solvent und woher stammt das Kapital?
- Welche Rolle spielen Vermittler, Berater und Exporteure?
- Ist das Umfeld politisch beeinflusst?
- Kann die Sicherheit der Mitarbeiter vor Ort garantiert werden?

Hier setzt das Due Diligence Investigation an. Durch Vor-Ort-Recherchen könne nach Auffassung von Jan Blume-Werry von KDM-Sicherheitsconsulting sichergestellt werden, dass Unternehmen ihre Risiken minimieren können, indem an sich nicht absehbare Gefahren, im Vorfeld identifiziert werden. Vor allem erhalten Unternehmen gerichtsverwertbare Beweise, die im Falle eines Prozesses verwertbar sind.

Wie ein DDI-Prozess konkret aussieht, finden Sie in den Folien von Jan Blume-Werry (http://www.lexisnexis.de/events/compliance-day-2015/due-diligence-investigations-kdm.pdf).

Literaturempfehlung zu Compliance
Eine Herausforderung für jede internationale Unternehmung sind trotz weltweiter Harmonisierungsbemühungen die unterschiedlichen Rechtslagen und die Rechtspraxis bei Compliance-Verstößen. Das Handbuch Compliance International (http://www.compliancedigital.de/ce/handbuch-compliance-international/ebook.html) gibt einen einzigartigen Überblick über die Grundlagen compliance-relevanter Rechtsgebiete bedeutender Wirtschaftsnationen.
Wie Sie ein erfolgreiches Internes Kontrollsystem (IKS) aufbauen um wirtschaftlichen Schaden abzuwenden, Vorgaben effizient zu erfüllen und letztlich den Wert des Unternehmens zu steigern, zeigt Oliver Bungartz in dem Handbuch Interne Kontrollsysteme (IKS) (http://www.compliancedigital.de/ce/handbuch-interne-kontrollsysteme-iks-7/ebook.html). Neben nationalen Vorgaben betrachtet Bungartz auch internationale Vorgaben – wie z. B. die Regelungen nach dem sog. China-SOX und zum Outsourcing nach IDW PS 951 n.F.

PinG neu auf COMPLIANCEdigital

Nachricht vom 03.07.2015

Zuwachs! Die Zeitschrift Privacy in Germany (PinG) ergänzt das eJournal-Angebot von COM-

PLIANCEdigital um das wichtige Thema Datenschutz und Compliance.

Big Data, Industrie 4.0, Cyber Security und Datenschutz sind nur einige Schlagworte, deren Bedeutung für Compliance-Verantwortliche in den letzten Jahren immer wichtiger wurde. Compliance ohne fundierte Kenntnisse zu Datenschutz und Co. ist nach Überzeugung von Datenschutzexperten undenkbar.

Die rasanten Entwicklungen im Bereich Datenschutz und Compliance beleuchtet seit 2013 der Herausgeber Prof. Niko Härting gemeinsam mit den Autoren der Zeitschrift Privacy in Germany (PinG) und in Zusammenarbeit mit dem Vorstand der Stiftung Datenschutz. Sechs Ausgaben pro Jahr garantieren eine schnelle und fundierte Versorgung mit aktuellen und relevanten Informationen rund um das Thema Datenschutz und Compliance.

Ab sofort steht die Zeitschrift für Datenschutz und Compliance den Lesern und Abonnenten von COMPLIANCEdigital zur Verfügung.

Was ist PinG?

- Die Zeitschrift PinG richtet sich an alle, die sich mit der praktischen Umsetzung von Datenschutz und Compliance im Unternehmen befassen – ob rein rechtlich oder wissenschaftlich.
- PinG wendet sich an alle, die digitale Kommunikation als selbstverständlich begreifen und im Alltag aktiv nutzen.
- PinG beleuchtet und analysiert das Thema Privacy mit dem internationalen Blick auf das Geschehen durch Beiträge von Autoren aus aller Welt.
- Ping ist intermedial. Die Autoren berichten auf allen Kommunikationskanälen über die rasanten Entwicklungen: gedruckt, als eJournal, per Blog, Twitter und Youtube – und nun auch auf COMPLIANCEdigital.
- PinG bietet ein breites Meinungsspektrum und lässt alle zu Wort kommen, die Wichtiges zum Thema beitragen können: Insider, Experten ... und selbstverständlich auch die Leser!

Perfekte Ergänzung

Mit dieser Ausrichtung ergänzt PinG das eJournal-Angebot von COMPLIANCEdigital perfekt. Insgesamt stehen den Lesern und Abonnenten nun – neben den über 200 eBooks – insgesamt sieben Fachzeitschriften zur Verfügung:

- NEU: Privacy in Germany (PinG) (http://www.compliancedigital.de/short/ping/ejournal-inhalt.html)
- Risk, Fraud & Compliance (ZRFC) (http://www.compliancedigital.de/short/zrfc/ejournal-inhalt.html)
- Journal of Business Compliance (http://www.compliancedigital.de/short/buco/ejournal-inhalt.html)
- WiJ – Journal der Wirtschaftsstrafrechtlichen Vereinigung e.V. (http://www.compliancedigital.de/short/wij/ejournal-inhalt.html)
- Zeitschrift für Corporate Governance (ZCG) (http://www.compliancedigital.de/short/zcg/ejournal-inhalt.html)
- Zeitschrift Interne Revision (ZIR) (http://www.compliancedigital.de/short/zir/ejournal-inhalt.html)
- News-Magazin Zeitschrift für Compliance (ZfC) (http://www.compliancedigital.de/short/zfc/ejournal-inhalt.html)

Inhalte der aktuellen Ausgabe von PinG (4/2015)

Die aktuelle Ausgabe (4/2015) geht der Frage nach, wie die richtige Balance zwischen Freiheit und Sicherheit in einem Rechtstaat gefunden werden kann?

- Cyberwar – eine reale Gefahr aus der virtuellen Welt (http://www.compliancedigital.de/ce/cyberwar-eine-reale-gefahr-aus-der-virtuellen-welt/detail.html) (Dr. Hans-Georg Maaßen)
- "My Phone is my Castle" – Legal Implications for the Search and Seizure of Cell Phones by Law Enforcement Officials in the U. S. A. and Germany (http://www.compliancedigital.de/ce/my-phone-is-my-castle-legal-implications-for-the-search-and-seizure-of-cell-phones-by-law-enforcement-officials-in-the-u-s-a-and-germany/detail.html) (Henning Hofmann, Alexander Seidl, Ferdinand Wessels)
- Scoring – was ist zulässig und welche (Auskunfts-)Rechte haben die Betroffenen? Überblick zum aktuellen Stand der Rechtsprechung (http://www.compliancedigital.de/ce/scoring-was-ist-zulaessig-und-welche-auskunfts-rechte-haben-die-betroffenen/detail.html) (Dr. Wulf Kamlah, Stefan Walter)
- Fragen zur Vorratsdatenspeicherung: Interview mit OStA Christoph Frank, Bundesvorsitzender des Deutschen Richterbundes (DRB) (http://www.compliancedigital.de/ce/fragen-zur-vorratsdatenspeicherung/detail.html)
- Aus Sicht der Stiftung Datenschutz – Die elektronische Patientenakte – auf das Wie kommt es an (http://www.compliancedigital.de/ce/aus-sicht-der-stiftung-datenschutz-die-elektronische-patientenakte-auf-das-wie-kommt-es-an/detail.html) (Frederick Richter)