Creditreform
Compliance Services

Compliance & Risk Newsletter

Ausgabe 3/2017

September 2017

Inhaltsverzeichnis

Fachartikel: Compliance Management-Systeme	2
Fachartikel: Überblick zum Internen Kontrollsystem (IKS)	7
Fachartikel: Keine verdeckte Gewinnausschüttung riskieren	11
Fachartikel: Die unendliche Geschichte endet doch – Jetzt ist Schluss mit der Störerhaftung!	13
Fachartikel: Personalausweiskopie jetzt datenschutzrechtlich zulässig!	15
News: Transparenzregister	17
Impressum	18

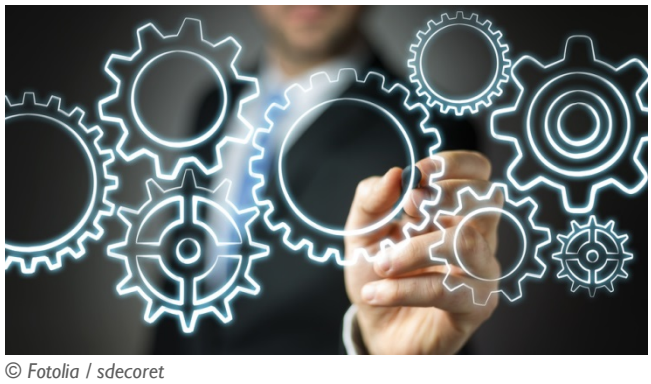
Compliance Management-Systeme

Gesetzliche Grundlage und Bedeutung

Die Einhaltung von Gesetzen, Richtlinien, Verordnungen, vertraglichen Pflichten und unternehmensinternen Leitlinien ist neben der Verfolgung von Good Practice-Standards von besonderer Bedeutung für einen nachhaltigen Unternehmenserfolg. Compliance als integraler Bestandteil der Corporate Governance bedeutet aufgrund der steigenden rechtlichen Anforderungen, der erhöhten Sensibilität der Öffentlichkeit sowie der strafrechtlichen Verfolgung von Compliance-Verstößen eine verstärkte Herausforderung für Verantwortungsträger in Unternehmen.

Das deutsche Recht sieht bis heute keine faktische Verpflichtung zur Implementierung von Compliance Management-Systemen für Unternehmen vor, die nicht den Mindestanforderungen an das Risikomanagement (MaRisk) oder den Mindestanforderungen an die Compliance-Funktion (MaComp) unterliegen. Jedoch lässt sich eine mittelbare Verpflichtung durch die den gesetzlichen Vertretern von Unternehmen obliegende allgemeine Legalitätsverantwortung herleiten, die die Einhaltung rechtlicher Vorgaben zwingend vorschreibt. Diese ergibt sich insbesondere aus dem Aktiengesetz (nachfolgend AktG), dem GmbH-Gesetz (nachfolgend GmbHG) oder dem Gesetz über Ordnungswidrigkeiten (nachfolgend OWiG) wie folgt:

Gemäß § 91 Abs. 2 AktG hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Weiter legen §§ 76, 93 AktG und auch § 43 GmbHG fest, dass die Unternehmensleitung zur Abwendung vermeidbarer Schäden von der Gesellschaft verpflichtet ist. Darüber hinaus ist gemäß § 107 Abs. 3 Satz 2 AktG eine Überwachung der Wirksamkeit des Rechnungslegungsprozesses, des internen Kontrollsystems, des Risikomanagementsystems, der internen Revision sowie der Abschlussprüfung vorgesehen. Diese nicht abschließende Aufzählung wird durch § 130 OWiG ergänzt, der festlegt, dass sich die gesetzlichen Vertreter eines Unternehmens, die Aufsichtsmaßnahmen unterlassen, die erforderlich sind, um Zuwiderhandlungen zu verhindern, ordnungswidrig verhalten.



© Fotolia / sdecoret

Die Erfüllung der dargestellten Compliance-Anforderungen obliegt im Grundsatz stets den gesetzlichen Vertretern und dem Aufsichtsorgan. Diese Verantwortung lässt sich auch nicht durch eine Auslagerung delegieren.

Unternehmen, die nicht die Anforderungen der MaRisk oder MaComp erfüllen müssen, gehören regelmäßig der Industrie-, Handels- und Dienstleistungsbranche an. Für diese gibt der Prüfungsstandard des Instituts der Wirtschafts-

prüfer IDW PS 980 ein Rahmenwerk zur Einhaltung von rechtlichen Vorgaben sowie Selbstverpflichtungen im Rahmen eines unternehmensspezifischen Compliance Management-Systems vor. Darüber hinaus erfolgt hierdurch sowohl eine Dokumentation der eigenen Compliance-Standards als auch die Formulierung von Compliance-Anforderungen an die Geschäftspartner.

Begriffsbestimmungen

Die vorherrschende Definition von Compliance umfasst zum einen die Einhaltung rechtlicher Vorgaben sowie die Vorhaltung von Vorkehrungen zum Entgegenwirken von Risiken, die sich aus der Nichteinhaltung dieser Vorgaben ergeben können. Darüber hinaus berücksichtigt Compliance auch die Einhaltung unternehmensinterner Regelungen und Selbstverpflichtungen sowie Fragestellungen der Unternehmensethik und Nachhaltigkeit.

Die Gesamtheit der zur Einhaltung rechtlicher Vorgaben sowie unternehmensinterner Regelungen definierten Grundsätze und Maßnahmen, die auf Grundlage der von den gesetzlichen Vertretern definierten Ziele festgelegt werden, wird als Compliance Management-System bezeichnet.

Die definierten Grundsätze und Maßnahmen zielen auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie ggf. Dritter ab und sollen auf die Verhinderung von Compliance-Verstößen hinwirken. Die Struktur und der Aufbau eines Compliance Management-Systems im Sinne des IDW PS 980 werden in den nachfolgenden Ausführungen dargestellt.

Grundelemente eines Compliance Management-Systems nach IDW PS 980

1. Compliance-Kultur

Die Compliance-Kultur stellt die Grundlage für die Angemessenheit und Wirksamkeit des Compliance Management-Systems dar. Sie wird vor allem durch die Grundeinstellungen und Verhaltensweisen der gesetzlichen Vertreter des Unternehmens sowie durch die Rolle des Aufsichtsorgans („Tone at the Top") geprägt. Die Compliance-Kultur beeinflusst die Bedeutung, die die Mitarbeiter des Unternehmens der Beachtung von Regeln beimessen und damit die Bereitschaft zu regelkonformem Verhalten.

2. Compliance-Ziele

Die gesetzlichen Vertreter legen auf Grundlage der allgemeinen Unternehmensziele sowie einer Analyse und Gewichtung der für das Unternehmen bedeutsamen Regeln die Ziele fest, die mit dem Compliance Management-System erreicht werden sollen. Insbesondere umfasst dies auch die Festlegung der relevanten Teilbereiche und der einzuhaltenden Regeln. Die Compliance-Ziele stellen die Grundlage für die Beurteilung von Compliance-Risiken dar.

3. Compliance-Risiken

Unter Berücksichtigung der Compliance-Ziele werden die Compliance-Risiken festgestellt, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der Compliance-Ziele zur Folge haben können. Hierzu ist ein Verfahren zur systematischen Risikoerkennung und –berichterstattung zu implementieren. Die fest-

gestellten Risiken werden im Rahmen eines Risk Assessments im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Auswirkungen (z.B. Schadenshöhe) analysiert.

4. Compliance-Organisation

Das Management regelt die Funktionen, Rollen, Verantwortlichkeiten sowie die Aufbau- und Ablauforganisation im Rahmen des Compliance Management-Systems als integraler Bestandteil der Unternehmensorganisation und stellt die für ein wirksames Compliance Management-System notwendigen Ressourcen zur Verfügung.

5. Compliance-Programm

Basierend auf der Beurteilung der Compliance-Risiken werden Grundsätze und Maßnahmen eingeführt, die auf die Begrenzung der Compliance-Risiken und damit auf die Vermeidung von Compliance-Verstößen ausgerichtet sind. Das Compliance-Programm umfasst auch die bei festgestellten Compliance-Verstößen zu ergreifenden Maßnahmen und ist angemessen zu dokumentieren.

6. Compliance-Kommunikation

Die jeweils betroffenen Mitarbeiter und ggf. Dritte werden sodann über das Compliance-Programm sowie die festgelegten Verantwortlichkeiten informiert, damit sie ihre Aufgaben im Compliance Management-System ausreichend verstehen und sachgerecht erfüllen können. Berichtswege im Unternehmen werden definiert und festgelegt.

7. Compliance-Überwachung und Verbesserung

Naturgemäß ist es mit der bloßen Errichtung eines Compliance Management-Systems nicht getan – dies muss vielmehr fortwährend überwacht und ggf. an aktuelle Entwicklungen angepasst werden. Voraussetzung für die Überwachung und Verbesserung ist eine ausreichende Dokumentation des Compliance Management-Systems. Werden im Rahmen der Überwachung systemische Schwachstellen oder Compliance-Verstöße identifiziert, sind diese an die gesetzlichen Vertreter des Unternehmens zu berichten. Die gesetzlichen Vertreter sind für die Durchsetzung des Compliance Management-Systems sowie die Beseitigung der Mängel und die Verbesserung des Systems verantwortlich.

Individualisierung des Compliance Management-Systems

Diese sieben Grundelemente sind nicht als starre Anforderungskriterien oder Messgrößen zu verstehen, sondern als Rahmenkonzept, welches dem Unternehmen gewisse Handlungs- und Gestaltungsspielräume belässt, um das Compliance Management-System speziell auf die unternehmensspezifischen Anforderungen auszurichten. Zudem stehen die genannten Grundelemente in Wechselwirkung zueinander. Ein Compliance Management-System sollte demnach unter Berücksichtigung des vorgegebenen Rahmenkonzeptes individuell und bedarfsgerecht an die Unternehmensbedürfnisse im konkreten Einzelfall angepasst werden.

Hierbei gilt es, die Rechtsform und Größe des Unternehmens, die Art der Geschäftsaktivitäten und deren Risikogehalt sowie weitere unternehmensspezifische Besonderheiten zu berücksichtigten. Darüber hinaus ist die Bestimmung der relevanten Teilbereiche des Compliance Management-Systems ein wichtiger Parameter für dessen Angemessenheit und Wirksamkeit. Neben der Korruptionsvermeidung über die Beachtung zollrechtlicher Vorgaben können der Datenschutz, die Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen, das Kartell- und Wettbewerbsrecht, aber auch rechtliche Bestimmungen zum Umweltschutz wichtige Teilbereiche des Compliance Management-Systems sein.

Diese bedarfsgerechte Individualisierung ist zur Vermeidung von Compliance-Verstößen und sonstigen Verfehlungen sowie zur Reduzierung von Vermögens- und Reputationsrisiken durch Verletzung rechtlicher Vorgaben, erforderlich.

Zur Sicherstellung der Einhaltung der für das Unternehmen relevanten gesetzlichen Vorgaben sowie der von den gesetzlichen Vertretern festgelegten internen Regelungen sind im Rahmen des unternehmensspezifischen Compliance-Management-Systems angemessene und wirksame Grundsätze und Verfahren festzulegen. Diese zielen auf ein verantwortungsvolles und gesetzeskonformes Verhalten der gesetzlichen Vertreter und Mitarbeiter des Unternehmens, insbesondere gegenüber der Öffentlichkeit, Umwelt, Geschäftspartner sowie Kunden und sonstigen Interessengruppen wie z.B. Stake- und Shareholdern des Unternehmens, ab. Die angemessene und wirksame Ausgestaltung des Compliance Management-Systems ist unter Berücksichtigung der Unternehmenswerte regelmäßig zu überprüfen.

Obwohl eine individuelle Ausrichtung des Compliance Management-Systems erforderlich ist, haben sich in den letzten Jahren Standards etabliert, die einer Vielzahl von Systemen zugrunde liegen. Diese umfassen insbesondere die nachfolgenden Punkte:

- Identifizierung und Systematisierung von Compliance-Anforderungen und -Risiken,
- Festlegung von Compliance-Standards in Form eines Code of Conduct und sonstiger Richtlinien,
- Festlegung von Zuständigkeiten und Funktionen im Rahmen des Compliance Management-Systems,
- Information und Schulung der Mitarbeiter als Präventivmaßnahmen,

- Einrichtung von Kontrollhandlungen zur Überwachung der Einhaltung von Compliance-Anforderungen,
- Implementierung eines standardisierten Prozesses zum Umgang mit Compliance-Verstößen,
- Regelmäßige Berichterstattung der Compliance-Verantwortlichen an die gesetzlichen Vertreter und den Aufsichtsrat des Unternehmens.

Fazit

Die gesetzlichen Vertreter und Aufsichtsorgane von Unternehmen sollten der gesteigerten Bedeutung, die der Erfüllung von Compliance-Standards und -Anforderungen zukommt, durch die Vorhaltung entsprechender Sicherungssysteme Rechnung tragen. Die Implementierung eines Compliance Management-Systems unterstützt die gesetzlichen Vertreter von Unternehmen bei der Wahrnehmung dieser Verantwortung.

Relevante Risiken werden durch ein angemessenes und wirksames Compliance Management-System frühzeitig erkannt und an geeignete Stellen berichtet, sodass diesen rechtzeitig begegnet werden kann, um negative Auswirkungen für das Unternehmen zu verhindern. Compliance sollte nicht nur als notwendige regulatorische Anforderung gesehen werden, sondern auch als Möglichkeit, das Vertrauen in die Integrität und Seriosität des Unternehmens zu fördern und somit die Reputation des Unternehmens nachhaltig zu verbessern.

(Kristin Kramer, Fachreferentin Compliance und Geldwäscheprävention, Creditreform Compliance Services GmbH)

Überblick zum Internen Kontrollsystem (IKS)

Was ist der Sinn und Zweck des „Internen Kontrollsystems“ innerhalb eines Unternehmens?

Vorstand und Aufsichtsrat eines Unternehmens benötigen transparente und verlässliche Informationen über die Wirksamkeit des Internen Kontrollsystems, um strategische Risiken zu erkennen und adäquat durch die Hinterlegung von Maßnahmen steuern zu können. Zu diesem Zweck wird innerhalb des jeweiligen Unternehmens ein institutionalisiertes und systematisches Verfahren eingeführt (Überwachungsprozess für das Interne Kontrollsystem).

Bezogen auf Kreditinstitute lassen sich sowohl die Notwendigkeit zur Einrichtung eines Internen Kontrollsystems, als auch die daraus resultierenden Anforderungen an dessen Wirksamkeit, im Wesentlichen aus dem Kreditwesengesetz (KWG), den Mindestanforderungen an das Risikomanagement (MaRisk) sowie dem Bilanzrechtsmodernisierungsgesetz (BilMoG) ableiten.

Was genau wird unter einem „Internen Kontrollsystem“ verstanden?

Das Interne Kontrollsystem hat als Zielsetzung die Sicherstellung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen) sowie die Einhaltung der maßgeblichen rechtlichen Vorschriften.

Das Interne Kontrollsystem umfasst somit alle Grundsätze, Verfahren und Maßnahmen, die auf dieses Ziel hinwirken. Da sich das Interne Kontrollsystem auf alle Geschäftsprozesse des Unternehmens richtet, trägt es zur Einhaltung der unternehmerischen Ziele bei.

© Fotolia / Melpomene

Was bedeutet das Three Lines of Defence-Modell und welche Funktion haben dabei die einzelnen Verteidigungslinien?

Der Überwachungsprozess für das IKS eines Kreditinstitutes besteht aus 3 Säulen und orientiert sich an dem Modell der „Drei Verteidigungslinien einer ordnungsgemäßen Geschäftsorganisation“. Die jeweiligen Verteidigungslinien haben dabei folgende Aufgaben und Verantwortungsbereiche:

Säule 1 (1. Verteidigungslinie), Fachbereich:

Die erste Verteidigungslinie ist unmittelbar bei den operativ tätigen Geschäftsbereichen angesiedelt. Diese sind im Rahmen ihres bereichsinternen Kontrollsystems (IKS) dafür verantwortlich, ihre Risiken zu identifizieren und zu dokumentieren. Sie haben hierfür angemessene Prozesse und Maßnahmen zu implementieren

(z. B. Arbeitsanweisungen, Schulung der Mitarbeiter, Kontrollen), um die bestehenden Risiken zu minimieren bzw. auszuschalten.

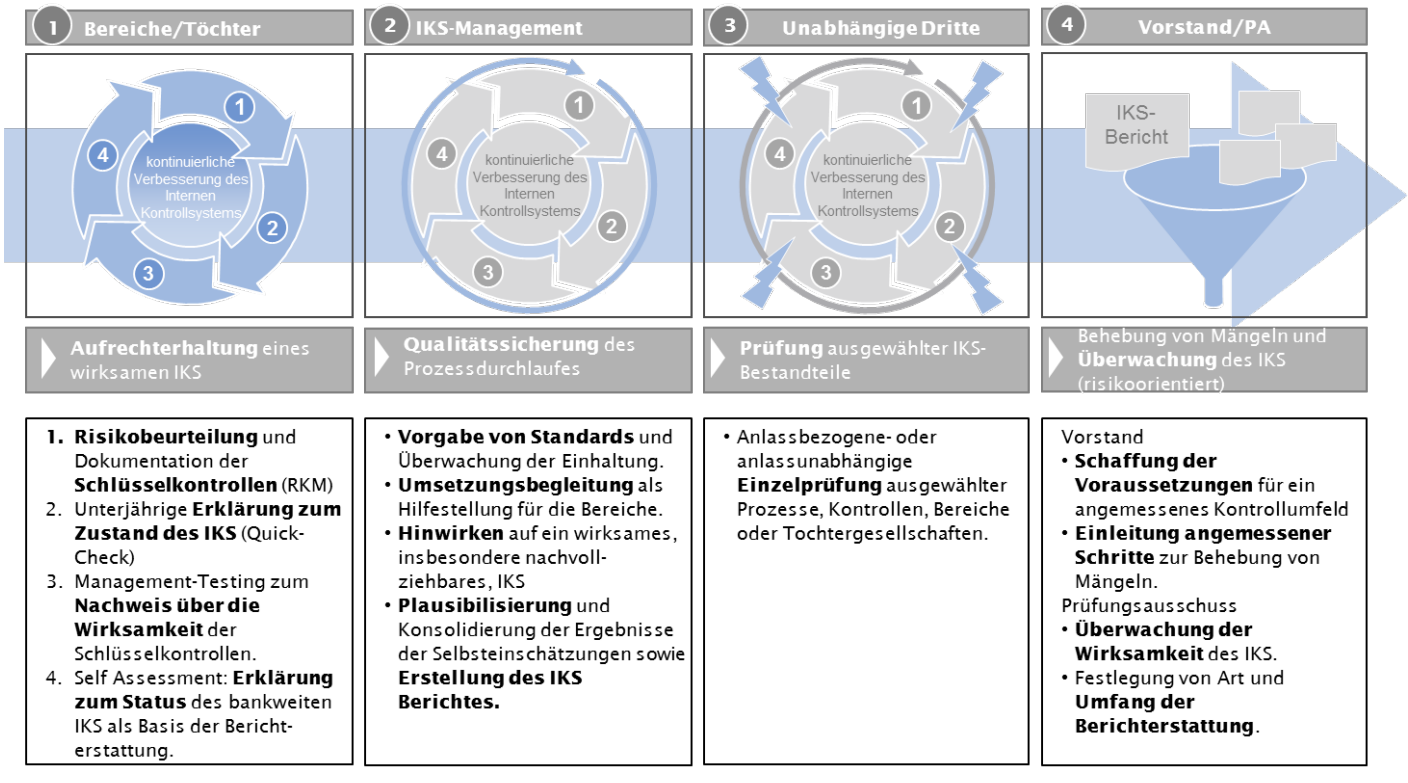
Säule 2 (2. Verteidigungslinie), IKS-Management:

Der zweiten Verteidigungslinie – hierzu gehört beispielsweise im Rahmen seiner Zuständigkeiten unter anderem auch Compliance – obliegt es, die operativ tätigen Geschäftsbereiche zu beraten und zu überwachen. Ebenso etabliert Compliance regelmäßige und anlassbezogene Kontrollen, hierzu gehören insbesondere die Überwachung der Selbstkontrollen der 1st Line of Defence.

Säule 3 (3. Verteidigungslinie), Unabhängige Dritte:

Die dritte Verteidigungslinie besteht aus der internen Revision eines Unternehmens. Ihre Aufgabe als prozessunabhängige Einheit ist es, die Aufsichtsgremien bei der Überwachung und Kontrolle bestehender und potenzieller Risiken durch eine unabhängige Bewertung des Risikomanagements und des Kontrollsystems zu unterstützen. Sie bewertet unabhängig die Wirksamkeit der Steuerungs- und Überwachungsprozesse und prüft unabhängig von den Bereichen die Wirksamkeit des IKS.

Das folgende Schaubild verdeutlicht das Zusammenspiel der einzelnen Säulen und Verantwortungsbereiche:



Was bedeutet das für die Mitarbeiter eines Kreditinstituts bei der Ausübung Ihrer operativen Tätigkeit?

Innerhalb des jeweiligen operativen Arbeitsumfeldes bestehen unterschiedlich stark ausgeprägte Prozessrisiken. Sofern diese Risiken bzw. prozessuale Schwachstellen als ‚wesentlich' eingestuft werden, müssen ausreichend ausgestaltete, wirksame Kontrollhandlungen (sogenannte Schlüsselkontrollen) definiert werden. Als Wesentlichkeitskriterien können u. a. Transaktionsvolumen, Anzahl aufgetretener Schadensfälle und die zum konkreten Prozessschritt zugeordnete Risikokategorie herangezogen werden. Diese wesentlichen Risiken und Kontrollhandlungen sind Bestandteil des IKS-Überwachungsprozesses einer Bank. Alle wesentlichen und unwesentlichen Risiken mit den dazugehörigen Kontrollhandlungen bilden insgesamt das Interne Kontrollsystem der Unternehmung.

Ziel ist es, das wesentliche Risiko zu minimieren bzw. komplett zu mitigieren. Die darauf ausgerichteten Kontrollhandlungen sind in Verantwortung der zuständigen Organisationseinheit (d.h. durch den Prozessowner) durch diese direkt zu integrieren. Nicht ausreichend ausgestaltete Kontrollhandlungen haben zur Folge, dass Risiken nicht oder nur teilweise beherrscht werden.

Kontrollaktivitäten treten innerhalb des Unternehmens auf allen Ebenen und in allen Funktionen auf. Neben der Funktionstrennung bzw. dem Vier-Augen-Prinzip werden Kontrollaktivitäten im Wesentlichen durch Eingabe- und Freigabesysteme, Schnittstellenüberwachungen und manuelle Kontrollen in Form von Plausibilisierungen und Vergleichen auf Prozessebene durchgeführt. Wichtig in diesem Zusammenhang ist die für einen sachverständigen Dritten nachvollziehbare Dokumentation.

Wann ist eine Kontrollhandlung wirksam?

Eine Kontrollhandlung ist dann wirksam, wenn sie angemessen und funktionsfähig ist.

- Angemessen ist eine Kontrolle, wenn durch sie der angestrebte Zweck erreicht werden kann und ihre Intensität dem Risikogehalt des Vorgangs entspricht.
- Funktionsfähig ist eine Kontrolle, wenn sie entsprechend der Kontrollbeschreibung durchgeführt wird.

Warum kommen auf die jeweiligen IKS-Verantwortlichen der Fachbereiche im Zuge der Durchführung bestimmter Kontrollhandlungen erhöhte Dokumentationspflichten zu?

Die Grundlage für die Selbsteinschätzung der Fachbereiche eines Unternehmens (das sog. Self Assessment) bilden die den Anforderungen des IKS-Überwachungsprozesses entsprechend dokumentierten Kontrollhandlungen.

In einer Stichprobenziehung erfolgt durch einen über die Fachbereichsleitung beauftragten Management Tester eine Aussage zur Wirksamkeit des fachbereichsinternen Kontrollsystems. Diese Wirksamkeitsaussagen werden durch die zweite Verteidigungslinie, die zum Beispiel IKS-Management genannt werden kann gemeinsam mit dem zuständigen Fachbereich plausibilisiert.

Das Ergebnis dieser Plausibilisierung ist die Basis für die jährliche IKS-Berichterstattung an den Prüfungsausschuss und den Vorstand. Das IKS-Management ist der Ansprechpartner (Beratung und Überwachung) in Sachen IKS.

In welchem Zusammenhang stehen die verschiedenen Ansätze zur Risikobetrachtung?

In einem Unternehmen befassen sich verschiedene Einheiten mit unterschiedlichen Risiken. Diese Risiken werden in getrennten Prozessen erfasst und ausgewertet. Alle existierenden Risikoarten und deren Kontrollen sind Bestandteil des Internen Kontrollsystems. Die innerhalb des IKS als prozessuale Risiken dokumentierten Risiken lassen sich daher in die einzelnen Risikoarten, u.a. in operationelle Risiken oder strategische Risiken aufteilen. Das Prozessrisiko kann sich somit aus unterschiedlichen Risikoarten zusammensetzen. Ziel des IKS-Überwachungsprozesses ist es dabei, die angemessene Kontrolle aller wesentlichen Risiken sicherzustellen. Hierzu gehört auch, transparent zu machen, welche unterschiedlichen Risiken bzw. Risikoarten mit einem Prozess verbunden sind.

Wie wird der IKS-Prozess an die zukünftigen unternehmensexternen und –internen Entwicklungen angepasst?

Eine ständige Verbesserung und Optimierung des Internen Kontrollsystems und des IKS-Überwachungsprozesses ist für das IKS-Management von zentraler Bedeutung. Die Digitalisierung wird zukünftig auch im IKS-Überwachungsprozess über die Einführung von DV-Lösungen in den Unternehmen Einzug halten. Das bedeutet eine spürbare Veränderung im Prozess der Kontrollhandlungen (bei der Kontrolldefinition –durchführung, -dokumentation), d.h. in der Arbeitsumgebung der Kontrollverantwortlichen, beispielsweise über eine papierlose Kontrolldokumentation.

Eine weitere Entwicklung in Bezug auf den IKS-Überwachungsprozess ist eine zunehmende Verzahnung innerhalb der einzelnen Risikomanagement-Systeme, z.B. die Verlinkung von prozessualen Risiken, die im IKS identifiziert, bewertet und gesteuert werden, mit operationellen Risiken aus dem Risikocontrolling-Prozess des Unternehmens.

(RA Hartmut T. Renz, Group Chief Compliance Officer, Direktor / Managing Director Compliance, Landesbank Baden-Württemberg | Djordje Kristijan Sirca MSc., IKS-Management: Beratung und Überwachung der Organisationseinheiten zum Themenkomplex Internes Kontrollsystem, Landesbank Baden-Württemberg | Diplom-Betriebswirt (FH) Markus Wurster, IKS-Management: Beratung und Überwachung der Organisationseinheiten zum Themenkomplex Internes Kontrollsystem, Landesbank Baden-Württemberg)

Keine verdeckte Gewinnausschüttung riskieren

An die Geschäftsführer-Vergütung in mittelständischen Unternehmen werden immer strengere Maßstäbe angelegt. Immer häufiger steht der Vorwurf einer verdeckten Gewinnausschüttung im Raum. Welche Risiken drohen und was Firmen tun können.

Die Geschäftsführer-Vergütung vieler Unternehmen steht auf unsicherem Terrain. Zum einen schränken neue Gerichtsurteile den Gestaltungsfreiraum weiter ein. Zum anderen leiten Betriebsprüfer bei Verdacht auf eine verdeckte Gewinnausschüttung häufiger ein Strafermittlungsverfahren ein. Inhabergeführte Unternehmen sollten das Thema Geschäftsführervergütung dringend auf den Prüfstand stellen, rät die Wirtschaftskanzlei WWS in Mönchengladbach. So können Unternehmen steuerliche Tretminen erkennen und umgehen.

GmbH, KG auf Aktien oder AG: Betriebsprüfer nehmen die Geschäftsführer-Vergütung von inhabergeführten Kapitalgesellschaften besonders kritisch unter die Lupe. Hierzu hinterfragen sie anhand eines Drittvergleichs Art und Höhe der Geschäftsführer-Vergütung. Vermeintlich überhöhte Leistungen an Gesellschafter-Geschäftsführer werten sie schnell als verdeckte Gewinnausschüttung (vGA). Die Folge sind hohe Steuernachzahlungen samt Zinsen, mitunter auch saftige Bußgelder oder Geldstrafen. „Neben dem Grundgehalt nehmen Betriebsprüfer verstärkt Extras wie Tantiemen, Pensionszusagen oder Sachbezüge ins Visier“, sagt Torsten Lambertz, Wirtschaftsprüfer und Steuerberater der WWS. „Kritische Finanzbeamte haben schnell Einwände, da Gehaltsbestandteile oft großen Interpretationsspielraum bieten.“

© Fotolia / Sebastian Duda

Die jüngere Rechtsprechung lässt Betriebsprüfer künftig noch tiefer schürfen. Rückendeckung bieten ihnen etwa zwei Urteile des Bundesfinanzhofs. Gegenstand ist in beiden Fällen ein Mietvertrag zwischen einer GmbH und ihrem Gesellschafter-Geschäftsführer zu strittigen Konditionen (BFH, Az. I R 8/15, Az. I R 12/15). Obwohl die vereinbarte Miete dem ortsüblichen Mietspiegel entsprach, vertreten die Richter die Auffassung, dass es sich um eine vGA handelt. Maßgeblich ist für die Entscheidung, dass die Miete nicht kostendeckend und keine Gewinnerzielung möglich war. „Firmen sollten die Miethöhe nicht nur auf Basis von Mietspiegeln festlegen, sondern bei der Ermittlung der Kostenmiete auch immer die Zweite Berechnungsverordnung nach dem Zweiten Wohnungsbaugesetz heranziehen“, rät WWS-Steuerberater Lambertz. „Zudem darf ein angemessener Gewinnaufschlag von rund fünf Prozent im Mietvertrag nicht fehlen.“

Einen weiteren Ansatzpunkt bietet Betriebsprüfern ein Urteil zum Verrechnungskonto für Gesellschafter (FG München, Az. 7 K 531/15). Ein GmbH-Gesellschafter-Geschäftsführer hatte private Ausgaben vom GmbH-Konto bezahlt. Die Zahlungen glich der Firmenchef jedoch nicht aus. Über die Jahre häuften sich Verbindlichkeiten auf über eine halbe Million Euro an. Für die Richter liegt eine vGA vor, da der Geschäftsführer für das geliehene Geld keine Zinsen zahlte. In ähnlich gelagerten Fällen sollten Unternehmen immer Zinszahlungen in angemessener Höhe vereinbaren. „Sofern die Gesellschaft selbst einen Kredit zu ihrer Refinanzierung aufgenommen hat, sollten die hierfür fälligen Zinsen als Maßstab für die Verzinsung des Geschäftsführer-Kredits herangezogen werden“, rät WWS-Experte Lambertz. „Andernfalls ist der marktübliche Zinssatz maßgeblich.“

Auch beim Thema Einlagenrückgewähr ist erhöhte Vorsicht geboten. Entsprechende Leistungen an ihre Gesellschafter müssen Kapitalgesellschaften nach amtlich vorgeschriebenem Muster bescheinigen. Die Bescheinigung einer Einlagenrückgewähr kann nach Bekanntgabe des Feststellungsbescheids nicht mehr erfolgen. Dies gilt nach Auffassung des Sächsischen Finanzgerichts selbst dann, wenn eine vGA erst im Rahmen einer Betriebsprüfung nachträglich festgestellt und aus diesem Grund keine Bescheinigung ausgestellt wurde (FG Sachsen, Az. 2 K 1860/15). Die Finanzrichter räumen jedoch den Finanzämtern die Möglichkeit ein, im Einzelfall zugunsten des Steuerpflichtigen zu entscheiden. Einen Rechtsanspruch können Betroffene hieraus aber nicht herleiten. Wegen der grundsätzlichen Bedeutung des Falles wurde die Revision vor dem Bundesfinanzhof zugelassen.

Wie können Kapitalgesellschaften eine vGA von vornherein vermeiden? Firmen sollten bestehende und neue Vergütungsvereinbarungen hinsichtlich formaler Kriterien und der Höhe prüfen. Entscheidend ist bei der Vergütung immer die Frage, ob sie ein gewissenhafter Firmenchef auch einem Nichtgesellschafter gewähren würde und ob sie der Höhe nach marktüblich ist. Unternehmen sollten grundsätzlich für den Fremdvergleich aktuelle Gehaltsstudien heranziehen. Sicherheitshalber sollten Firmen mit ihrem Steuerberater alle Gestaltungsmodelle durchgehen, um steuerliche Knackpunkte zu beseitigen.

(Torsten Lambertz, Wirtschaftsprüfer und Steuerberater der Kanzlei WWS Wirtz, Walter, Schmitz in Mönchengladbach)

Die unendliche Geschichte endet doch – Jetzt ist Schluss mit der Störerhaftung!

Nachdem die Bundesregierung bereits im letzten Jahr – ohne Erfolg – versucht hatte, die sog. „Störerhaftung“ abzuschaffen, scheint es nun endlich vollbracht zu sein. Schon Ende Juni beschloss der Bundestag den umstrittenen Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes (TMG). Dieser wurde nun, zwei Tage vor der Bundestagswahl, auch vom Bundesrat gebilligt. Das sogenannte WLAN-Gesetz tritt am Tag nach seiner Verkündung in Kraft, was nach Angaben des Bundeswirtschaftsministeriums Ende November 2017 der Fall sein könnte.

Im Kern bedeutet die Gesetzesänderung, dass Anbieter von WLAN-Hotspots ab sofort nicht mehr dafür haftbar gemacht werden können, wenn Dritte über ihren Internetzugang Rechtsverstöße (bspw. Urheberrechtsverstöße in Form von illegalen Film- bzw. Musikdownloads) begehen. Dasselbe Ziel verfolgte schon die zweite Änderung des TMG im Jahr 2016, die ihren Zweck allerdings deshalb verfehlte, weil man damals versäumt hatte, festzulegen, dass die Haftungsfreistellung von WLAN-Anbietern auch den Unterlassungsanspruch der Rechteinhaber umfasst. Diese Regelungslücke bot der Abmahnindustrie genügend Raum, um ihre durchaus lukrativen Geschäftsmodelle fortzuführen. Doch damit soll jetzt Schluss sein, denn die aktuelle Änderung schließt explizit auch die Unterlassungsansprüche im Rahmen der Störerhaftung aus.

Für viele ist dieser Schritt mehr als überfällig, da es in Deutschland weit weniger frei zugängliche WLAN-Hotspots gibt als in den meisten anderen Ländern der Welt, so dass man in der Vergangenheit bereits von der „WLAN-Wüste Deutschland“ oder dem „digitalen Entwicklungsland Deutschland“ sprach. Das hört man in Regierungskreisen freilich äußerst ungern. Im Übrigen stellte die Störerhaftung weltweit ein juristisches Unikum dar und war längst nicht mehr zeitgemäß.

© Fotolia / ra2 studio

Zwar ist diese Entwicklung selbstverständlich zu begrüßen, so bleibt ein gewisser Beigeschmack nicht aus. Denn, um die Inhaber von Urheberrechten nicht schutzlos zu stellen, hat die Regierung als Alternative die Möglichkeit von Netzsperren eingeräumt. Das bedeutet, dass die Urheberrechtsinhaber von den WLAN-Betreibern die Sperrung gewisser Inhalte fordern können, um wiederholte Urheberrechtsverletzungen zu vermeiden. Die Tragweite dieser Möglichkeit für die Praxis ist aktuell noch nicht abzusehen, so dass hier Rechtsunsicherheit bestehen bleibt. Allerdings müssen zumindest die Kosten solcher Maßnahmen die Rechteinhaber selbst tragen. Weiter ergeben sich für die Betreiber der öffentlichen Hotspots

diverse datenschutzrechtliche Fragestellungen, die es zu lösen gilt. Auch ein Passwortschutz ist mit der Gesetzesänderung überflüssig geworden, ebenso wie die Verpflichtung, von den Nutzern eine Registrierung zu verlangen. Fraglich ist also auch hier, ob überhaupt noch – und wenn ja, in welchem Maße – personenbezogene Daten der Nutzer verarbeitet werden.

Das Fazit der Gesetzesänderung könnte lauten „keine Verbesserung ohne Verschlechterung", denn durch die Möglichkeit der Netzsperren bleibt Rechtsunsicherheit bestehen. Wie sich dies in der Praxis entwickeln wird bleibt abzuwarten.

(Benjamin Spallek, LL.M,.Consultant Compliance und Datenschutz, Creditreform Compliance Services GmbH)

Personalausweiskopie jetzt datenschutzrechtlich zulässig!

Was schon lange Zeit gängige Praxis war, wird nun – dankenswerterweise – auch vom Gesetzgeber legitimiert!

Nach der alten Rechtslage war das Anfertigen von Personalausweiskopien nur in einem sehr eng abgesteckten Rahmen erlaubt. Als Beispiel sind hier insbesondere geldwäscherechtlich relevante Sachverhalte zu nennen, die den Verantwortlichen von Gesetzes wegen, konkret gemäß § 8 Abs. 2 des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG) dazu verpflichten, im Rahmen der Identifizierung des Vertragspartners Kopien von Ausweisen zu erstellen und aufzubewahren.

Doch die gesetzlichen Schranken hielten selbst öffentliche Stellen nicht davon ab, Personalausweiskopien zu verlangen, diese selbst anzufertigen oder die Ausweise für gewisse Zeit einzubehalten. Diese Vorgehensweise war Teil des Tagesgeschäfts.[1]

Nun hat der Gesetzgeber mit der Änderung des § 20 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG) auf diesen Umstand reagiert. Mit der Anpassung der Vorschrift an die tatsächlichen Gegebenheiten des Unternehmensalltags hat er auf einem über lange Zeit juristisch umstrittenen Gebiet für mehr Rechtssicherheit gesorgt.

Zwar ergibt sich aus der Gesetzesänderung eine deutlich weniger restriktive Rechtslage, allerdings kann nicht einfach „drauf los kopiert“ werden. Es gibt noch immer bestimmte Voraussetzungen, die erfüllt sein müssen, um das Kopieren eines Personalausweises zu legitimieren. So darf gemäß § 20 Abs. 2 PAuswG nur der Ausweisinhaber selbst, oder eine andere Person mit seiner Zustimmung, die Ablichtung durchführen. Außerdem muss die Ablichtung eindeutig und dauerhaft als Kopie kenntlich gemacht werden. Die Kenntlichmachung der Ablichtung kann beispielsweise durch deren Erstellung in schwarz-weiß oder einem deutlich sichtbaren Vermerk „Kopie“ erfolgen. Ergänzend sind natürlich die allgemeinen Anforderungen des Datenschutzrechts zum Umgang mit personenbezogenen Daten zu beachten. Das bedeutet, dass die sich aus der EU-Datenschutz-Grundverordnung (EU-DSGVO) und dem neuen Bundesdatenschutzgesetz (BDSG 2018) ergebenden Bestimmungen zusätzlich eingehalten werden müssen. Für die weitere Verwendung der Kopie gilt wiederum, dass nur der Ausweisinhaber zu deren Weitergabe berechtigt ist und er für die Verarbeitung von aus dem Personalausweis erhobenen personenbezogenen Daten seine Einwilligung erteilen muss. Um wirksam zu sein, muss sich auch die Einwilligungserklärung an den geltenden datenschutzrechtlichen Standards (Freiwilligkeit, Informiertheit, etc.) messen lassen.

Der vom Gesetzgeber verwendete Begriff *„Ablichtung“* ist neu und wird im Gesetz selbst

[1] dieDatenschützer Rhein Main, <https://ddrm.de/jobcenter-mainarbeit-offenbach-hessischer-datenschutzbeauftragter-beurteilt-scannen-und-kopieren-von-personalausweisen-als-nicht-von-der-rechtslage-gedeckt/>, besucht am 21.09.17.

nicht näher definiert. Begrüßenswert ist allerdings, dass die entsprechende Gesetzesbegründung hierzu eine konkrete Definition beinhaltet:

„Die genannten Handlungsformen – Fotokopieren, Fotografieren und Einscannen – werden unter dem abstrakten Begriff des Ablichtens zusammengefasst, das Ergebnis wird als Ablichtung bezeichnet.“[2]

Besonders erfreulich ist hieran, dass vom Oberbegriff der Ablichtung nun auch das seinerzeit besonders umstrittene Einscannen umfasst und folglich gestattet ist.

© *Fotolia / stadtratte*

Hingegen nicht vollständig geklärt ist, ob es erlaubt ist, die Ablichtung weitergehend zu bearbeiten und zu verändern. Insbesondere gewinnt diese Frage an Relevanz, wenn der Ausweisinhaber Stellen schwärzen möchte, weil er sie nicht offenbaren will und sie für den konkreten Einzelfall – seiner Meinung nach – irrelevant sind. Aus rein datenschutzrechtlicher Sicht ist das Schwärzen von für den Sachverhalt überflüssigen Datenfeldern freilich generell empfehlenswert, da es dem Grundsatz der Datenminimierung Rechnung trägt. Indessen hat die BaFin im Rahmen der geldwäscherechtlichen Identifizierungspflichten ein Schwärzen der – vermeintlich – nicht relevanten Ausweisdaten explizit für unzulässig erachtet. Dies wird aus der in § 8 Abs. 2 GwG normierten Pflicht abgeleitet, die zur Identifizierung des Vertragspartners notwendigen Dokumente **vollständig zu kopieren** und dies zu dokumentieren.

Zusammengefasst kann festgehalten werden, dass die Gesetzesänderung begrüßenswert ist, da der Gesetzgeber nun die Rechtslage der faktisch schon seit langem gelebten Unternehmenspraxis angepasst hat. Hierdurch sollten Rechtsunsicherheiten im Umgang mit der Kopie von Ausweisdokumenten der Vergangenheit angehören. Aus Perspektive der Datenschützer wäre überdies eine Klarstellung bezüglich einer Erlaubnis zur teilweisen Schwärzung der Ablichtungen wünschenswert.

(Benjamin Spallek, LL.M,.Consultant Compliance und Datenschutz, Creditreform Compliance Services GmbH)

[2] BT Drs. 18/11279.

Transparenzregister

Das Transparenzregister wurde mit den Änderungen im Geldwäschegesetz im 26. Juni 2017 eingeführt.

Bis zum 01. Oktober 2017 sind im Transparenzregister die Daten zum wirtschaftlich Berechtigten zu hinterlegen, sofern sich diese nicht bereits aus einem öffentlichen Register ergeben. Wichtig ist, dass diese Daten beim Register elektronisch geführt werden.

Meldungen an:
http://www.transparenzregister.de

Hier finden Sie auch weitere Informationen sowie eine Kurzanleitung.

Wer sind die Verpflichteten?

- Juristische Personen des Privatrechts (z.B. AG, GmbH, UG)
- Vereine
- Genossenschaften
- Stiftungen
- Europäische Aktiengesellschaften
- Eingetragene Personengesellschaften (z.B. OHG)

Unter bestimmten Voraussetzungen sind auch Trusts bzw. Treuhänder nicht rechtsfähiger Stiftungen verpflichtet Angaben zu den jeweiligen wirtschaftlich Berechtigten einzuholen, aufzubewahren sowie bis zum 01. Oktober 2017 in das Transparenzregister einzumelden.

Welche Daten müssen bei der Eintragung des wirtschaftlich Berechtigten angegeben werden?

- Vor- und Nachname
- Geburtsdatum
- Wohnort
- Art und Umfang des wirtschaftlichen Interesses (z.B. Kapitalbeteiligung, Stimmrechte) des wirtschaftlich Berechtigten

Wann muss nicht gemeldet werden?

Wenn sich die Angaben zu den wirtschaftlich Berechtigten bereits aus anderen öffentlichen Quellen oder Registern, wie

- Handelsregister,
- Partnerschaftsregister,
- Genossenschaftsregister,
- Vereinsregister,
- Liste der Gesellschafter (bei elektronischer Hinterlegung im Register)

ergeben, dann entfällt eine Meldeverpflichtung.

Wenn die Gesellschafterliste beim Handelsregister vorliegt, aber nicht elektronisch hinterlegt wurde, dann ist eine Meldung erforderlich.

Verstöße gegen die Eintragungspflicht können mit Bußgeldern geahndet werden.

Weitergehende Informationen können dem Merkblatt der IHK Berlin entnommen werden.
https://www.ihk-berlin.de/

Impressum

Herausgeber

Creditreform Compliance Services GmbH

Hellersbergstraße 11

41460 Neuss

Tel: +49 2131 109-1089

Fax: +49 2131 109-81089

www.creditreform-compliance.de

info@creditreform-compliance.de

Amtsgericht Neuss HRB 4213

USt-IdNr.: DE120690803

Geschäftsführung

Silvia Rohe

Redaktion, Layout und Satz

Julia Mohr

Weitere Autoren dieser Ausgabe

Kristin Kramer, Torsten Lambertz, Hartmut T. Renz, Djordje Kristijan Sirca, Benjamin Spallek, Markus Wurster

Bildnachweis

fotolia

Redaktioneller Hinweis