WIRTSCHAFTS campus
Dr. Peemöller GmbH

Fachgebiet:

Grundlagen der IT-Compliance

Lehrbrief 1

- ↗ **Definition Compliance und IT-Compliance**
- ↗ **Rechtliche Grundlagen**
- ↗ **Organisatorische Grundlagen**
- ↗ **Corporate Governance und Compliance**
- ↗ **Ethik-Kodex**

Verfasser:
Dipl.-Kfm. Dr. Silke Peemöller, Steuerberaterin
Prof. Dr. Volker H. Peemöller
Dipl.-Ing. Alban Seeholzer

Dr. Peemöller GmbH
Austraße 42
97299 Zell

Certified IT-Compliance Officer

Fernlehrgang

Stand: 2023

Lernziel:

Inhalt dieses Lehrbriefs sind die wesentlichen Grundlagen von Compliance. Sie werden deshalb mit den verschiedenen Definitionsansätzen vertraut gemacht und klären dabei die Abgrenzung zwischen traditioneller Unternehmens-Compliance (Corporate Compliance) mit der IT-Compliance.

Einen Überblick, welche Inhalte sich hinter Compliance verbergen, werden Sie im anschließenden Kapitel erhalten. Ausführlich werden die organisatorischen Fragen zur Compliance behandelt. Dazu wird die Frage diskutiert, wie die Funktion Compliance im Unternehmen zugeordnet werden kann und welche Unterstellungsmöglichkeiten infrage kommen.

Im Abschnitt über Corporate Governance und Compliance wird eine kurze Standortbestimmung der Begriffe vorgenommen und gezeigt, dass Corporate Governance die Regeln vorgibt und Compliance dafür sorgen soll, dass die Regelungen eingehalten werden.

Im Abschluss wird die Erforderlichkeit eines Ethik-Kodexes und die Anforderungen an den IT-Compliance Officer aufgezeigt.

Alle Abschnitte enthalten Kontrollfragen, um Sie mit der Thematik vertraut zu machen.

Wir wünschen Ihnen viel Erfolg bei der Bearbeitung!

Literatur

Abkürzungen

2. Definition

2.1 Definition „Compliance“

Definition „Compliance“

Sie haben schon die übliche Definition von Compliance kennengelernt: Einhaltung von Gesetzen, Vorschriften, Regeln und Plänen. Die von den Unternehmen einzuhaltenden Regelungen sind unzählig und reichen von A wie Arbeitssicherheit bis Z wie Zoll. Zum Teil werden deshalb nur spezielle Themen unter dem Begriff Compliance behandelt. Zu diesen speziell rechtlichen Themen zählen Geschäftspartnerprüfung, Geldwäsche, Korruption und Kartellrecht, Qualitätssicherung, Rückrufaktionen und Bilanzierung.

Diese Fragen wurden im Unternehmen bereits weitgehend organisiert und durch verschiedene Bereiche erledigt.

- Buchhaltung: Bilanzierung und GoB
- Steuerabteilung: Steuern und Zölle
- Rechtsabteilung: Kartellrecht und Korruption
- Personalabteilung: Arbeitssicherheit, AGG, Sozialabgaben usw.
- Datenschutzbeauftragter, DPO: Schutz personenbezogener Daten
- Informationssicherheitsbeauftragter, CISO: Schutz von Informationen
- Investor Relations: Publizität
- Interne Revision: Prüfung des innerbetrieblichen Kontrollsystems und des Risikomanagementsystems.

AGG
DPO
CISO

Es ist deshalb zu entscheiden, welcher Compliance-Ansatz gewählt werden soll. Ein sehr enger Ansatz stellt die rechtlichen Fragen in den Vordergrund. Die Themen werden wie bisher von den entsprechenden Stellen im Unternehmen bearbeitet und unter Compliance zusammengefasst. Wesentliche Sachverhalte sind dann:

enger Ansatz

- Verhinderung strafbaren Verhaltens
- Verhinderung von Regelverstößen von Mitarbeitern
- Einhaltung von Regeln, deren Verletzung zu schwerwiegenden Nachteilen führt (Strafen, Verhaftungen, Bußgelder, Reputationsverluste)

Daraus ergibt sich eine sehr enge Definition von Compliance, die hier nicht weiterverfolgt werden soll.

Definition nach DCGK

Der Deutsche Corporate Governance Kodex (DCGK) enthält ebenfalls eine Definition zum Compliance (Grundsatz 5):

„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance). Das interne Kontrollsystem und das Risikomanagementsystem umfassen auch ein an der Risikolage des Unternehmens ausgerichtetes Compliance Management System.“ DCGK 27.06.2022
Diese Definition nimmt eine Erweiterung um die unternehmensinternen Richtlinien vor. Es wird nicht nur an den Sanktionen angesetzt, sondern an der Beachtung der Vorgaben. Wie diese Beachtung erreicht wird, ob durch Sanktionen oder durch Integration der Mitarbeiter, bleibt dem Unternehmen vorbehalten.

Auffassung des IDW

Eine ähnliche Auffassung wird vom Institut der Wirtschaftsprüfer in Deutschland (IDW) vertreten: „Compliance – Einhaltung von Regeln (gesetzliche Bestimmungen und unternehmensinterne Richtlinien).“ IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980 vom 28.09.2022). Dazu wird unter der Textziffer (Tz.) A8 weiter ausgeführt: „Interne

Richtlinien des Unternehmens können auch von Dritten entwickelte Prinzipien oder Konventionen sein, zu deren Einhaltung sich das Unternehmen selbst verpflichtet hat."

Daraus leiten wir folgende Definition für Compliance ab:

Definition für „Compliance"

Der Begriff Compliance umfasst die Gesamtheit aller **Maßnahmen**, die das **regelkonforme Verhalten** eines Unternehmens, seiner Leitungs- und Überwachungsorgane sowie seiner Mitarbeiter im Hinblick auf die **gesetzlichen Ge- und Verbote** sowie die internen Richtlinien begründen. Wir verstehen Compliance als Bestandteil der Corporate Governance (ordnungsgemäßer Unternehmensführung).

Maßnahmen

Maßnahmen zu entwickeln ist eine betriebswirtschaftliche Aufgabe, da eine Reihe von Wahlmöglichkeiten existiert, wie die Einhaltung der Vorgaben im Unternehmen erreicht werden kann. In der Realität ist von unüberschaubaren Regelungen auszugehen; von unscharfen Abgrenzungen zwischen den beteiligten Personen und Institutionen und unterschiedlichen organisatorischen und strukturellen Regelungen. Die Entwicklung von Maßnahmen ist damit ein zeitaufwändiges und komplexes Unterfangen.

regelkonformes Verhalten

Regelkonformes Verhalten setzt Normen voraus, die den Personen bekannt und verständlich sind. Dazu gehören auch Regeln der Sanktionen, die bei Nicht-Einhaltung ergriffen werden. Damit gewinnen die Entwicklung, Kommunikation und Schulung bezüglich der Regelungen besonderes Gewicht.

gesetzliche Ge- und Verbote

Gesetzliche Ge- und Verbote sowie interne Richtlinien umfassen die sozialen Normen, denen sich ein Unternehmen stellen muss. Für die Organisationsmitglieder muss klar sein, welche Regelungen für den einzelnen gelten, und mit welchen Folgen die Nicht-Beachtung verbunden ist.

Selbst-verpflichtung

Selbstverpflichtung zur Compliance stellt einen Grundpfeiler dar. Die Unternehmensführung muss das Verhalten in der Organisation über ein Organisations- und Führungssystem steuern. Damit ist einmal zu erfassen, welche Möglichkeiten der Integration der Mitarbeiter bestehen, und in welchem Umfang ethische Ziele beachtet werden. Demgegenüber stehen der Umfang von Kontrollkosten und die Wahrscheinlichkeit der Aufdeckung von Regelverstößen. Zielsetzung ist es, unzulässige Handlungsweisen zu verhindern und Konformität mit vorgegebenen Verhaltensstandards herzustellen. Dies kann einmal durch Überwachung, Fremdkontrolle und Sanktionsmaßnahmen erfolgen. Es kann aber auch durch selbst bestimmte ethische Prinzipien ein eigenverantwortliches Handeln ermöglicht werden. Zwischen diesen beiden Ansätzen ist ein Ausgleich herzustellen.

-
-
-

2.2 Definition und Abgrenzung des Begriffes „IT-Compliance“

2.2.1 Definition „IT-Compliance“

Die Definition der IT-Compliance ist wenig überraschend der Definition der Unternehmens-Compliance ähnlich:

Bewusstsein

Kontrolle
Dokumentation

IT-Compliance bezeichnet die Kenntnis und Einhaltung sämtlicher regulatorischer Vorgaben und Anforderungen an das Unternehmen, die Initiierung und die Einrichtung entsprechender Prozesse und die Schaffung eines Bewusstseins der Mitarbeiter für Regelkonformität, sowie die Kontrolle und Dokumentation der Einhaltung der relevanten Bestimmungen gegenüber internen und externen Adressaten.[1]

Unternehmens-
schutz

IT-Compliance ist nicht nur ein Zustand, sondern ein Verhalten, das vorgabenkonformes und ethisches Handeln aller Beteiligten, einschließlich externer Partner impliziert. IT-Compliance ist eine Schutzfunktion, dient der Erhöhung der IT-Sicherheit und kann potenzielle Kosten durch Strafen und Reputationsschäden verhindern. [2]

Chancen

IT-Compliance erhöht auch Chancen auf Aufträge (Compliance Anforderungen von Ausschreibungen) oder ermöglicht erfolgreiche Geschäfte in Branchen mit regulatorischen Vorgaben (Kreditkartengewerbe, Automobilbranche, Finanzbranche, Versicherungswesen, KRITIS Branchen).

Gerade die Gewährleistung der IT-Sicherheit im Unternehmen, unabhängig der Größe oder Branche, liegt in primärer Linie im Aufgabenbereich der Geschäftsführung. Die IT-Sicherheit umfasst insbesondere:

- Prävention gegen externe Angriffe, insbesondere Cyberangriffe durch Hacker, Computerviren oder Botnets (ferngesteuerte Netzwerke von bereits infizierten Computern) oder Advanced Persistent Threat (APT), welche gerade großen Unternehmen, Institutionen oder Behörden durch den Einsatz von verschiedenen und vor allem individuellen „Waffen“ mit einer Erpressung finanziell schaden wollen
- Beachtung und Einhaltung der datenschutzrechtlichen Pflichten, wie zum Beispiel die DSGVO
- Regelmäßige Erstellung von Backups. Nach einem Urteil des Oberlandesgerichts Hamm vom 1. Dezember 2003 (Az. 13 U 133/03), welches bis heute gültig ist und angewendet wird, muss zum Beispiel eine Vollsicherung der Geschäftsdaten mindestens wöchentlich durchgeführt werden, da ansonsten bei eventuellen Schäden durch einen Datenverlust dem Unternehmen ein haftungsüberdeckendes Mitverschulden vorgeworfen werden kann.
- Erstellung bzw. Berücksichtigung von bereits vorhandenen Handlungsanleitungen, Best Practice-Vorgaben und bestehenden Standards im Segment der Wirtschaftsprüfung

Bei einer Nichtbeachtung einer oder mehrerer der oben genannten IT-Sicherheitsvorgaben seitens des Unternehmens drohen Strafen und Sanktionen wie zum Beispiel zivilrechtliche Ansprüche und Schadenersatzforderungen von Geschädigten gegenüber dem Unternehmen, deutliche Geldstrafen, Image- und Marketingschädigungen, ökonomische Nachteile zum Beispiel beim Kreditrating, die Aufkündigung und der Verlust des Versicherungsschutzes oder auch der Verlust bei der Ausschreibung und Vergabe von öffentlichen Aufträgen.

---

1 Vgl. Rath, M./Sponholz, R.: IT-Compliance, S. 27

2 Vgl. Knoll, H./Strahringer, S.: IT-GRC-Management, S. 19-20

Weiterhin können sowohl Aufsichtsräte als auch Vorstände und Geschäftsführer des angegriffenen und geschädigten Unternehmens persönlich in die Haftung genommen und zu teils sehr hohen Geldstrafen oder sogar Haftstrafen verurteilt werden.

Neue Technologien und unsachgemäße Anwendungen, gerade auch von Mitarbeitern, wie die Nutzung von Smartphones oder Tabletts während der Arbeitszeit im Unternehmen, Cloud Computing oder die fast ständige Online- Präsenz im Bereich Social Media (Facebook, Instagram) oder die Nutzung von Messengern (WhatsApp) und natürlich die strikte Einhaltung der DSGVO im Unternehmen beinhalten zusätzliche rechtliche Anforderungen und Risiken für ein Unternehmen.

Hier müssen durch den IT-Compliance Officer unternehmensinterne Regelungen im IT-Bereich und Verfahrensvorgaben zur IT-Sicherheit geschaffen und ständig aktualisiert werden. Beispiele dafür sind

- IT-Sicherheitsvorschriften
- E-Mail-Richtlinien
- Password-Richtlinien

Auch übergreifende Service-Level-Agreements zwischen den einzelnen Fachabteilungen im Unternehmen und der IT-Abteilung gehören zum direkten Aufgabenschwerpunkt eines IT-Compliance Officers.

Interne Regelwerke sind für die Compliance im Unternehmen aus zweierlei Hinsicht wichtig und relevant: Erstens dienen sie in vielen Fällen dazu, die strikte Befolgung aller anderen Regelwerke im Unternehmen sicherzustellen, indem sie eindeutige und immer aktuelle Handlungsanweisungen für die Mitarbeiter vorgeben.

Zum anderen dokumentieren die internen Regelwerke in der Außendarstellung des Unternehmens, dass vor allem rechtliche Vorgaben eingehalten und beachtet werden. Dies kann dem Unternehmen einen deutlichen Wettbewerbsvorteil gegenüber Konkurrenten auf dem Markt einbringen.

IT-Compliance erhöht daher auch Chancen auf Aufträge (Compliance Anforderungen von Ausschreibungen) oder ermöglicht erfolgreiche Geschäfte in Branchen mit regulatorischen Vorgaben (Kreditkartengewerbe, Automobilbranche, Finanzbranche, Versicherungswesen, KRITIS Branchen).

2.2.2 Abgrenzung des Begriffes „IT-Compliance“

Die IT-Compliance kann in vielerlei Hinsicht als ein wichtiges Teilgebiet der allgemeinen Compliance eines Unternehmens gesehen werden. Dies nicht zuletzt deshalb, weil inzwischen die meisten Arbeitsprozesse stark von der IT unterstützt werden. So gibt es kaum noch einen Vorgang, der heute nicht IT technisch erfasst und verwaltet wird. Egal ob Lohn- und Gehaltsabrechnung, Personalverwaltung, Kundenmanagement, Geschäftskorrespondenz oder die Warenwirtschaft, sämtliche Bereiche des modernen unternehmerischen Handels sind tief von der IT durchdrungen.

Teil der Corporate Compliance

Ohne eine funktionsfähige IT wären die meisten Betriebe heutzutage nach nur wenigen Tagen handlungsunfähig und möglicherweise sogar insolvent. Einen Ausfall zum Beispiel der Rechnungsverwaltung oder des Warenwirtschafssystems dürfte kaum ein größeres Unternehmen länger als ein paar Tage überleben. Bei großen Onlinehandelshäusern würde der Ausfall des Webservers für nur wenige Stunden bereits einen beachtlichen Millionenschaden durch entgangenen Umsatz und möglicherweise für immer verlorene Kunden nach sich ziehen. Der Diebstahl von Kundendaten durch einen erfolgreichen Hackerangriff könnte darüber hinaus zu einem erheblichen Imageschaden führen.

Beispiel: Cyberangriff auf die Suchmaschine Yahoo

Bereits im Dezember 2014 hatte Yahoo entdeckt, dass sich Hacker Zugang zu Benutzernamen, Passwörtern, E-Mail-Adressen, Telefonnummern, Geburtsdaten und Sicherheitsfragen von mindestens 500 Millionen Accounts verschafft hatten. Obwohl das Unternehmen über den Vorfall Bescheid wusste, informierte es die Nutzer nicht. Auch, dass die gleiche Hacker-Gruppierung noch bis Anfang 2016 Daten gestohlen hat, verschwieg Yahoo lange Zeit.

Im Sommer 2016 wurde dann bekannt, dass Yahoo mit Verizon in Übernahmeverhandlungen steht und der nächste Fehler folgte. Denn Yahoo unterrichtete Verizon zwar über Datenlecks, tat diese aber eher als geringfügig ab. Erst im September 2016 entschloss sich das Unternehmen dann dazu, den Vorfall gegenüber Verizon und der restlichen Öffentlichkeit publik zu machen.

Schon am nächsten Tag waren die Auswirkungen für Yahoo spürbar:

Der Aktienkurs des Unternehmens fiel um 3 %, der Börsenwert fuhr 1,3 Milliarden US-Dollar Verluste ein und die Nutzer fühlten sich hintergangen. Darüber hinaus zeigte sich natürlich auch Verizon nicht sonderlich erfreut über Yahoo's Handeln. Es kam zwar später noch zur geplanten Übernahme, Yahoo musste dafür aber den Kaufpreis um 350 Millionen US-Dollar vermindern.

Einen speziellen IT-Compliance Beauftragten gab es während der gesamten Zeit nicht im Unternehmen.

-
-
-