Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

Compliance-Struktur in Unternehmen

Antworten zu Fragen der Regelkonformität in Unternehmen – ein Leitfaden

www.itwirtschaft.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Inhalt

1 Einführung 3

2 Ziel des Leitfadens 3

3 Compliance: Was ist das? 5

3.1 Begriff “Compliance” 5

3.2 Notwendigkeit von Compliance 7

3.3 Funktionen von Compliance 7

3.4 Compliance-Aufgaben 9

4 Compliance: Rechtsgrundlagen 10

4.1 Allgemeine Rechtsgrundlagen 11

4.2 Besondere Anforderungen an Compliance 13

5 Compliance Organisation – Grundelemente 18

5.1 Überblick 18

5.2 Risikomanagement 19

5.3 Compliance-Kultur 21

5.4 Compliance-Kommunikation 24

5.5 Compliance-Organisation 25

5.6 Überwachung 26

6 Fazit 29

7 Kontakt 30

1 Einführung

Niemanden wird es überraschen zu hören, dass Compliance ein zentrales Thema für jedes Unternehmen darstellt. Das wissen Sie auch ohne besondere Hinweise. Was fraglich ist und bleibt, ist der Inhalt der Compliance:

Grundsätzlich richtet sich Compliance auf die **Einhaltung von allen anwendbaren Normen** in einem Unternehmen. In diesem Leitfaden unternehmen wir den Versuch, Compliance als ganzheitliches Managementbereich darzustellen, die Organisation der Regeleinhaltung im Unternehmen zu skizzieren und die notwendigen Elemente einer jeden funktionierenden Compliance zu beschreiben. Mithilfe dieses Leitfadens soll es Ihnen gelingen, die Compliance in Ihrem Unternehmen aufzubauen, zu verbessern und an die sich stetig ändernden Regelungen und Gegebenheiten anzupassen. Denn Compliance fordert jedes Unternehmen zu anhaltenden Prüfungen und Verbesserungen auf – denn nur so kann eine nachhaltige Regeleinhaltung gewährleistet werden.

2 Ziel des Leitfadens

Der Leitfaden zur Compliance, den Sie gerade auf Ihren Schirm haben oder in Ihren Händen halten, ist gewiss nicht der erste Compliance-Leitfaden in Deutschland. Warum sollten Sie also ausgerechnet diesen Leitfaden lesen?

Die Antwort ist ganz einfach – im Gegensatz zu vielen anderen Leitfäden in diesem Bereich wollen wir Ihnen ein Werkzeug in die Hand legen, welches Ihnen unmittelbaren Nutzen bringen kann. Wir widmen uns nicht einzelnen Rechtgebieten, einzelnen rechtlichen Fragen, die sicherlich eine sehr große Rolle im Unternehmensalltag spielen, und auch nicht einzelnen Bereichen des Wirtschaftens, die besondere Risiken bergen. Das Ziel dieses Leitfadens liegt gerade nicht darin, Ihnen die Rechtsgebiete oder Rechtsnormen darzustellen, die besonderer Aufmerksamkeit in Ihrem

Unternehmen bedürften, denn diese hängen maßgeblich von den Details und Besonderheiten eben Ihres Unternehmens ab. So kann etwa das Arbeitsrecht bei einem von zwei gleichberechtigen Gründer:innen geführten Unternehmen ohne Arbeitnehmer beinahe „ausgeblendet" werden. Ebenso keine Rolle dürfte das Wertpapier- und Börsenrecht in solchen Unternehmen spielen, die keinen Börsengang planen und sich selbst nicht mit Wertpapieren beschäftigen.

Zwar gibt es zahlreiche Rechtsgebiete, die für jedes einzelne Unternehmen von Bedeutung sind, wie etwa das Insolvenzrecht, das Gesellschaftsrecht, sobald mehr als nur ein:e Gründer:in vorhanden ist, das Wettbewerbs- und Kartellrecht oder das Produkthaftungsrecht.

Allerdings zielt dieser Leitfaden nicht darauf ab, aus Ihnen eine:n Expert:in in rechtlichen Fragen zu machen, sondern darauf, Ihnen die innere Organisation Ihres Unternehmens nahezubringen, die jeglichen Rechtsverstößen – egal aus welchem Rechtsgebiet – entgegenwirken soll. **Einer gut aufgebauten Compliance-Organisation** ist es nämlich weniger wichtig, um welche konkrete Rechtsnorm es sich handelt. Es geht **primär darum, klar zu definieren, wie genau die Einhaltung des Rechts in Ihrem Unternehmen sichergestellt werden kann**.

Sollten Sie nach konkreten Rechtsgebieten suchen, können wir Ihnen folgende Werke empfehlen:

- *Moosmayer, Compliance: Praxisleitfaden für Unternehmen, 4. Auflage 2021*
- *Wieland/Steinmeyer/Grüninger, Handbuch Compliance Management, 3. Auflage 2020*
- *Inderst/Bannenberg/Poppe, Compliance: Aufbau - Management - Risikobereiche, 3. Auflage 2017*
- *Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Auflage 2016*
- *Umnuß, Corporate Compliance Checklisten: Rechtliche Risiken im Unternehmen erkennen und vermeiden, 3. Auflage 2016*

3 Compliance: Was ist das?

Der Ausdruck Compliance wurde aus dem englischen Sprachgebrauch übernommen („*to comply*“, „*to comply with*“). Der Begriff „Compliance“ hat mehrere Übersetzungen, wie Einhaltung, Erfüllung, Übereinstimmung, Befolgung etc. Mediziner sprechen z.B. von Compliance, wenn es um die Einhaltung eines vom Arzt vorgeschriebenen Therapieplanes durch einen Patienten geht.

Eine Legaldefinition, also eine vom Gesetzgeber „vorgegebene“ im Gesetzestext niedergeschriebene Definition, von „Compliance“ existiert im deutschen Recht nicht. Daher ist der Begriff mit einer gewissen Unschärfe behaftet. Um dieser Unschärfe entgegenzuwirken, empfiehlt sich eine unternehmensinterne Definition der Compliance und der Maßnahmen, die diese umfassen soll.

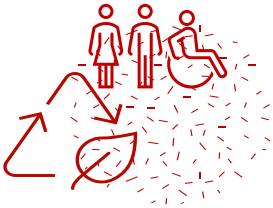
Im Allgemeinen geht es bei Compliance um die Einhaltung und Beachtung von Vorschriften, also im Wesentlichen um **Rechtstreue**. Darüber hinaus betrifft Compliance all die Maßnahmen, die die Einhaltung der Rechtsnormen absichern sollen.

3.1 Begriff “Compliance”

Versuchen wir nun den Begriff „Compliance“ zu definieren:

Compliance ist die Gesamtheit aller organisatorischen Aufsichts-, Schulungs- und Kontrollmaßnahmen der Geschäftsleitung, einschließlich der Einrichtung eines Berichts- und Dokumentationswesens, welche einen Verstoß des Unternehmens gegen gesetzliche Pflichten verhindern sollen.

Compliance bildet ein Bestandteil der „Corporate Governance“. Gemäß **DCGK** (Deutscher Corporate Governance Kodex) wird unter Corporate Governance der rechtliche und faktische Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens verstanden. Jedes Unternehmen soll dabei im Unternehmensinteresse geführt werden. Der DCGK verdeutlicht die Verpflichtung von Vorstand und Aufsichtsrat, im Einklang mit den Prinzipien der sozialen Marktwirtschaft unter Berücksichtigung der Belange der Aktionäre, der Belegschaft und der sonstigen mit dem Unternehmen verbundenen Gruppen (Stakeholder) für den Bestand des Unternehmens und seine nachhaltige Wertschöpfung zu sorgen (Unternehmensinteresse). Diese Prinzipien verlangen nicht nur **Legalität**, sondern auch ethisch fundiertes, eigenverantwortliches Verhalten (Leitbild des „Ehrbaren Kaufmanns“).



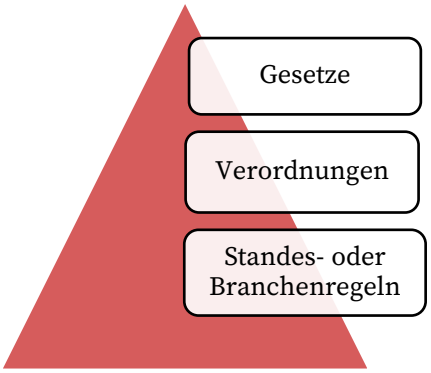
Wie der DCGK betont, haben sich das Unternehmen und seine Organe in ihrem Handeln der Rolle des Unternehmens in der Gesellschaft und ihrer gesellschaftlichen Verantwortung bewusst zu sein, weil Sozial- und Umweltfaktoren den Unternehmenserfolg beeinflussen und die Tätigkeiten des Unternehmens Auswirkungen auf Mensch und Umwelt haben. Dies soll bei der Führung und Überwachung im Rahmen des Unternehmensinteresses Berücksichtigung finden.

Unternehmensziel: betriebliche Leistung
Regelkonformes Verhalten – nur **untergeordnetes** Ziel (aus ökonomischer Perspektive)
ABER: Einhalten von Gesetzesnormen und unternehmensinternen Leitlinien ist Ausdruck unternehmerischer Entscheidung

Nach der Überarbeitung des DCGK lässt sich die Compliance im Grundsatz 5 finden. Dort heißt es:

> „Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance)“.

Compliance soll demensprechend auf den Prinzipien einer gesetzeskonformen und ethisch fundierten eigenverantwortlichen Unternehmensführung aufbauen. Sie umfasst dabei sämtliche Rechtsnormen und -grundsätze sowie die Regelwerke, die für ein Unternehmen kraft autoritativer Anordnung verbindlich sind, d.h. denen es sich nicht entziehen kann: Gesetze, Verordnungen und rechtlich verbindliche Standes- oder Branchenregeln.



Darüber hinaus gehören zu den zu beachtenden Rechtsvorschriften auch jene, die für ein bestimmtes Unternehmen aufgrund einer freiwilligen Unterwerfung bzw. Selbstverpflichtung verbindlich sind. Diese „freiwillig auferlegten Regeln“ beinhalten beispielsweise ethische oder andere Standards, die inhaltlich über die verbindlichen Gebote und Verbote des Gesetzgebers hinausgehen.

Es muss daher für jedes Unternehmen **individuell ermittelt** werden, welche (internationalen und nationalen) Gesetze, Verordnungen und übrigen Regeln sowie Standards usw. für das Unternehmen kraft autoritativer Anordnung und aber auch kraft Selbstverpflichtung maßgeblich und demnach einzuhalten sind.

Einen einheitlichen „One-Size-Fits-All“-Maßstab für Compliance gibt es nicht – und soll es auch nicht geben, denn **Compliance ist individuell** und von Unternehmen zu Unternehmen wegen der Größe, Art, Branche etc. sehr unterschiedlich.

3.2 Notwendigkeit von Compliance

Compliance als Maßnahmen für Regelkonformität sind – spätestens jetzt dürfte es klar sein – für jedes Unternehmen notwendig. Diese Notwendigkeit lässt sich durch folgende Punkte untermauern:

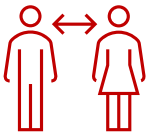
- Hohe Bußgelder für bestimmte Verstöße (Kartellrecht, Datenschutz)
- Rechtsprechung in Schadensersatzfällen schärfer geworden
- Rufschäden verbreiten sich in der digitalisierten Welt sehr schnell
- Aufsichts- und Strafverfolgungsbehörden sensibilisiert
- Öffentlichkeitsdruck (Transparenz)
- Unternehmenskultur als Wirtschaftsgut anerkannt
- Globalisierung (US Sentencing Guides, UK Bribery Act etc.)

3.3 Funktionen von Compliance

Compliance hat vier Hauptfunktionen: die Schutzfunktion, die Beratungsfunktion, die Überwachungsfunktion sowie die Imagefunktion.

- Die **Schutzfunktion** der Compliance richtet sich einerseits unmittelbar auf die Einhaltung von zwingenden Vorschriften durch Unternehmensangehörige und andererseits auf den Schutz des Unternehmens und seiner Stakeholder, ins besondere Mitarbeiter:innen, vor Schadensersatzansprüchen und sonstiger Haftung.

- Die **Beratungsfunktion** der Compliance umfasst das Informieren und Schulen von Unternehmensangehörigen in allen compliance-relevanten Bereichen, die Beratung der Geschäftsleitung beim Aufbau und Verbesserung der Compliance-Organisation sowie die Unterstützung aller Unternehmensangehörigen bei Änderung der Prozesse und Verfahren.



- Die **Überwachungsfunktion** der Compliance richtet sich auf die Überwachung von Regelungen und Maßnahmen, die organisationsintern implementiert worden sind, sowie auf die Aufklärung der Verstöße und Sanktionierung des Fehlverhaltens.

- Die **Imagefunktion** der Compliance hat zwei Dimensionen: eine interne, die sich darauf richtet, dass Unternehmensangehörige eine Bindung zum Unternehmen aufbauen und sich als Teil des Unternehmens wahrnehmen, was regelmäßig deren Regeleinhaltung stimuliert, sowie eine externe, die Kund:innen und Geschäftspartner:innen des Unternehmens adressiert und darauf gerichtet ist, das Ansehen des Unternehmens bei diesen Gruppen zu verbessern bzw. aufrecht zu erhalten.

Compliance-Funktionen

Schutzfunktion

- Einhaltung der rechtlichen Vorschriften
- Schutz des Unternehmens & der Mitarbeiter

Überwachungsfunktion

- Überwachung implementierter organisatorischer Regelungen

Beratungsfunktion

- Information und Schulung der Mitarbeiter

Imagefunktion

- intern (Identifikation der Mitarbeiter mit dem Unternehmen)
- extern (Ansehen bei Kunden, Geschäftspartnern etc.)

3.4 Compliance-Aufgaben

Die Aufgaben der Compliance ergeben sich praktisch aus deren Funktionen und umfassen die Beratung, die Interessenvertretung, die Prävention sowie die Ermittlungen.

Beratung (*Advisory*):

- Beratung der Geschäftsbereiche im Hinblick auf einschlägige Gesetze, Regelungen und Vorschriften
- Beratung der Geschäftsbereiche im Hinblick auf regulatorische Initiativen
- Regelmäßige Berichterstattung an Senior Management und Aufsichtsorgan zu Compliance-Themen
- Eskalation identifizierter Mängel und Probleme in Compliance-Angelegenheiten und Empfehlung geeigneter Abhilfemaßnahmen
- Regelmäßige Schulungen und Ausbildungsmaßnahmen für Mitarbeiter zu geltenden Regelungen und Vorschriften

Interessenvertretung (*Advocacy*):

- Kooperation mit Aufsichts- und anderen Behörden
- Ansprechpartner für Aufsichtsbehörden
- Koordination und Begleitung von aufsichtsbehördlichen Untersuchungen
- Beantwortung von Anfragen der Regulatoren und Aufsichtsbehörden
- Vertretung der Interessen der Bank im Rahmen von regulatorischen Initiativen
- Mitwirkung in Industriegruppen und Branchenverbänden

Prävention (*Prevention*):

- Erstellung und Kommunikation von Compliance-Grundsätzen, Richtlinien und Verfahren (Compliance-Regelwerk)
- Regelmäßige Schulungen und Ausbildungsmaßnahmen für Mitarbeiter zu geltenden Regelungen und Vorschriften
- Mitwirkung bei der Entwicklung neuer Produktideen („New Product Approval“)
- Begleitung der Neukundenannahme („New Client Adoption“)
- Unterstützung der Chinese Wall Organisation durch z.B.:
  - Führung von Watch- und Restricted List (Insiderverzeichnis)
  - Management von Interessenkonflikten (Clearing und Eskalation)
  - Begleitung des „Wall Crossing“-Verfahrens

Ermittlungen und Feststellungen (*Detection*), mithin Kontrolle und Überwachung interner Compliance-Regelungen:

- Überwachung von Transaktionen auf eigene Rechnung (Mitarbeitergeschäfte), Eigengeschäfte sowie Kundenkonten (Compliance Control Room)
- Vollständigkeitserklärungen zu Mitarbeitergeschäften (Drittinstitute)
- Überwachung der Meldung bedeutender Stimmrechtsanteile („Position Monitoring“)
- Durchführung regelmäßiger Prüfungen zur Überwachung von marktkonformem Verhalten, Market Conformity Control (MCC)
- Schulungsteilnahmen

4 Compliance: Rechtsgrundlagen

In you think compliance is expensive, try noncompliance.

Paul McNulty, former US Deputy Attorney General

Nach dieser Einführung, in der bereits die Bedeutung, die Funktionen und die Aufgaben der Compliance beschrieben worden sind, stellen sich drei wichtigsten Fragen, die beantwortet werden müssten, bevor im Unternehmen eine Compliance-Organisation aufgebaut wird:

WANN

kommt es zur Haftung?

WAS

kann unternommen werden um eine Pflicht-verletzung zu vermeiden?

WER

ist dafür zuständig?

Diese Fragen können nur beantwortet werden, wenn die rechtlichen Grundlagen der Compliance erläutert werden. Zum einen gibt es hierbei allgemeine Rechtsgrundlagen einer Compliance-Organisation zu betrachten, zum anderen müssten die Bereiche um Wissenszurechnung, Informationsmanagement und Delegation sowie „der sichere Hafen“ der Business Judgement Rule angeschaut werden.

4.1 Allgemeine Rechtsgrundlagen

Rechtsgrundlagen der Compliance lassen sich nicht in irgendeinem einzigen Gesetz finden, vielmehr sind sie über verschiedenste Normen des Straf-, Ordnungswidrigkeiten-, Gesellschaftsrechts sowie Normen zahlreicher anderer Rechtsgebiete verstreut. Die wichtigste Norm in diesem Kontext ist der erste Absatz des § 130 OWiG:

„Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterläßt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen."

Diese Rechtsnorm ist nicht unbedingt „nutzerfreundlich" formuliert. Gemeint ist Folgendes:

Jedes Unternehmen muss Aufsichtsmaßnahmen vornehmen, um bestimmte (nämlich mit Strafe oder Geldbuße bedrohte) Rechtsverstöße zu vermeiden. Dabei gibt es – in jedem Einzelfall individuell zu ermittelnde – Mindeststandards für absolut notwendige, „gehörige", Aufsichtsmaßnahmen. Werden diese weggelassen und kommt es dann zu einem solchen Verstoß, werden der Unternehmensträger selbst (also die GmbH, die AG, die OHG, der Kaufmann etc.) sowie seine Organe (Geschäftsführer:in, Vorstand etc.) in der Regel dafür haften müssen. Diese Norm hat viele Facetten, sorgt regelmäßig für neue Untersuchungen, Dissertationen und Forschungsprojekte und bildet zusammen mit § 9 OWiG und § 30 OWiG die Grundlage der Unternehmens- und Organhaftung für Verstöße der Unternehmensangehörigen.

Darüber hinaus sind die Aufsichtspflichten, mithin diese Pflicht zur Kontrolle des Verhaltens von unternehmensangehörigen, in gesellschaftsrechtlichen Vorschriften enthalten.

Ohne tief in die juristischen Einzelheiten einzusteigen, wollen wir an dieser Stelle betonen:

Jedes Unternehmen sowie seine Organe sind für das rechtskonforme Verhalten der Unternehmensangehörigen verantwortlich und entsprechende, stets individuelle, Maßnahmen müssen getroffen werden, um dieses zu gewähren.

§ 93 Abs. 1 AktG „Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder

„Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln. Über vertrauliche Angaben und Geheimnisse der Gesellschaft, namentlich Betriebs- oder Geschäftsgeheimnisse, die den Vorstandsmitgliedern durch ihre Tätigkeit im Vorstand bekanntgeworden sind, haben sie Stillschweigen zu bewahren."

§ 43 Abs. 1 GmbHG „Haftung der Geschäftsführer“

„Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.“

Alle börsennotierten Unternehmen müssen – über die Regelung des § 161 AktG – über die Einhaltung der Grundsätze des DCGK (Deutscher Corporate Governance Kodex) informieren oder erklären, warum diese nicht eingehalten werden. Der DCGK finden im Grundsatz 5 die Verpflichtung zur Compliance (s.o.). Dieses Dokument hat zwar lediglich für die genannten börsennotierten Gesellschaften eine normative Geltung, erstreckt aber seine Bedeutung auch auf solche Unternehmen, die dem DCGK „formell“ nicht verpflichtet sind, jedoch einen Wert auf transparente und nachvollziehbare Unternehmensführung legen.

Branchenspezifische und funktionsbezogene Compliance-Regelungen flankieren die allgemeinen Regeln. Zu nennen sind beispielsweise § 25 KWG für Kreditinstitute oder §§ 58 ff. WpHG für Wertpapierdienstleistungsunternehmen; Art. 30, 33, 35, 37 DSGVO bezüglich datenschutzrechtlicher oder § 12 AGG bezüglich gleichbehandlungsrechtlicher Pflichten etc. In international tätigen Konzernen sowie in Tochterunternehmen ausländischer Gesellschaften kommen noch entsprechende ausländische Normen und Verfahren hinzu, die ebenfalls Auswirkungen auf die Compliance-Organisation haben (müssen). Die Unternehmensleitung hat alle wesentlichen Entscheidungen über die Ausgestaltung der Compliance sowie der Implementierung eines Compliance-Managements selbst zu treffen und für die Überwachung der Wirksamkeit zu sorgen.

Diese Aufgaben kann die Unternehmensleitung einerseits horizontal, d.h. an ein bestimmtes Mitglied der Unternehmensleitung, als auch vertikal an einen Compliance-Beauftragten delegieren. Selbst wenn Aufgaben delegiert werden, ist die Unternehmensleitung jedenfalls zur Überwachung verpflichtet.

Es müssen nicht nur die für ein Unternehmen relevanten Normen eingehalten, auch muss die Einhaltung dieser Normen durch die Unternehmensleitung und beauftragte Mitarbeiter:innen auch überprüft werden. Durch eine funktionierende Compliance sollen Risiken regelwidrigen Verhaltens frühzeitig erkannt und darauf reagiert werden. Langfristig soll so jegliches Fehlverhalten eines Mitgliedes der Organisation oder des Unternehmens vermieden werden.

4.2 Besondere Anforderungen an Compliance

4.2.1 Wissenszurechnung und Informationsmanagement

Wissenszurechnung, also die Zurechnung von Informationen, die Unternehmensangehörige haben, dem Unternehmen selbst (so etwa wie „Weiß denn die Volkswagen AG von Manipulationen an der Abgas-Software?“) und die daraus folgende Notwendigkeit, Informationen und Informationsfluss im Unternehmen zu organisieren, bilden einen der Hauptpfosten der Compliance. Beide Bereiche – sowohl die Wissenszurechnung als auch das Informationsmanagement – sind typische Begleiterscheinungen des arbeitsteiligen Wirtschaftens.

Eine allgemeine gesetzliche Regelung der Wissenszurechnung findet sich in § 166 BGB:

„(1) Soweit die rechtlichen Folgen einer Willenserklärung durch Willensmängel oder durch die Kenntnis oder das Kennenmüssen gewisser Umstände beeinflusst werden, kommt nicht die Person des Vertretenen, sondern die des Vertreters in Betracht.

(2) Hat im Falle einer durch Rechtsgeschäft erteilten Vertretungsmacht (Vollmacht) der Vertreter nach bestimmten Weisungen des Vollmachtgebers gehandelt, so kann sich dieser in Ansehung solcher Umstände, die er selbst kannte, nicht auf die Unkenntnis des Vertreters berufen. Dasselbe gilt von Umständen, die der Vollmachtgeber kennen musste, sofern das Kennenmüssen der Kenntnis gleichsteht.“

Auch diese Vorschrift ist etwas kompliziert formuliert. Es geht – bezüglich eines Unternehmens – darum, dass das „Wissen“ eines Unternehmens (das natürlich nicht existieren kann, weil das Unternehmen lediglich ein juristisches Konstrukt ist) dem Wissen seiner Organe und anderer Unternehmensangehörigen, die dieses Unternehmen nach außen repräsentieren, gleichgestellt wird.

Dabei stellen sich – gerade im Unternehmenskontext – Fragen zum Wissensverlust und Wissensaufspaltung besonders scharf. Ebenso wichtig ist die Frage nach der Wissensverfügbarkeit (welches Wissen/welche Informationen an welcher Stelle des Unternehmens zu welchem Zeitpunkt noch verfügbar sein muss). Grundsätzlich gilt das Prinzip der Wissenszurechnung zu Lasten des Unternehmens, also muss sich das Unternehmen darum kümmern, dass wichtige Informationen auch gesammelt, gespeichert und abgerufen werden können. Aber auch die Organmitglieder haben hier besondere Vorsicht walten zu lassen: wegen der Organisationspflicht wird das im Unternehmen vorhandene Wissen regelmäßig ihnen zur Last gelegt. Auch wenn die früher geltende unbeschränkte Wissenszurechnung aufgegeben wurde und der sog. „wertenden Beurteilung“ Platz gemacht hat, ergibt sich allein aus den gesetzlichen Vorschriften und der richterlichen Auslegung und Konkretisierung die Pflicht eines jeden Unternehmens zur ordnungsgemäßen Organisation des Wissens bzw. der internen Kommunikation.

Was umfasst aber diese Wissensorganisationspflicht?

Sie umfasst:

- Wissensweiterleitung – jede:r Unternehmensangehörige:r muss wissen, welche Informationen in welchem Umfang wann an wen weitergegeben werden müssen
- Wissensbeschaffung – Entscheidungen im Unternehmen sind anhand ausreichender Informationen zu treffen; dafür muss bestimmt werden, welche Informationen für welche Entscheidung notwendig sind, wie diese zu beschaffen sind und wie das Ganze zu dokumentieren ist
- Wissensspeicherung – vorhandene Informationen müssen sortiert, kategorisiert und strukturiert gespeichert werden, damit sie auch später zugänglich bleiben

Informationsmanagement:

Informationsmanagement muss daher grundsätzlich so „breit und tief“ wie möglich sein. Das Unternehmen soll ersuchen, alle Informationen, die notwendig erscheinen – entweder für die bereits vorhandene Situation oder für die Zukunft oder im Hinblick auf die Vergangenheit (Stichwort Dokumentation) – strukturiert zu managen. Das Informationsmanagement ist allerdings nicht grenzenlos: Auch hier gibt es drei wichtige Schranken, die sich aus dem Gedanken der Gleichstellung eines Unternehmens einem Menschen (der doch durchaus Sachen vergessen kann oder für unwichtig halten kann oder falsche Entscheidungen wegen nicht-ausreichender Informationen treffen kann) ergeben:

persönliche Schranke

- Was ist der Anlass der Information?

inhaltliche Schranke

- Welche Informationen werden typischerweise aktenmäßig festgehalten?

zeitliche Schranke

- Speicherungsdauer: Wie lange soll eine Information sinnvollerweise gespeichert werden?

Zusätzliche Grenzen ergeben sich aus Betriebs- und Geschäftsgeheimnissen, dem Datenschutz, dem Insiderwissen und anderen Rechtsmaterien.

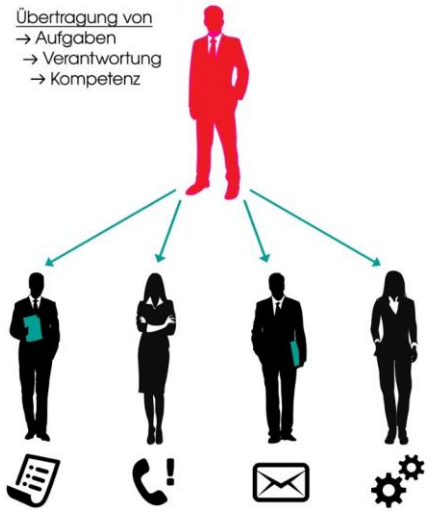
4.2.2 Delegation im Unternehmen

Das deutsche Recht bürdet die Allzuständigkeit und die Gesamtverantwortung den Vertretungsorganen auf. Diese sind also für alles im Unternehmen zuständig, tragen aber auch für alles im Unternehmen die Verantwortung.

Dennoch ist die Delegation, mithin die Übertragung bestimmter Aufgaben oder Aufgabenbereichen, prinzipiell erlaubt, allerdings mit folgenden Besonderheiten:

- Gesamtverantwortung ist NICHT delegierbar
- Fremdes Verschulden wird nicht zugerechnet (Vertretungsorgane, also die Geschäftsleitung, würde also im Falle eines Verstoßes gegen gesetzliche Normen nicht für den Verstoß selbst haften, sondern lediglich für die Vernachlässigung der eigenen Überwachungspflicht – so wie die Eltern nicht für die Verfehlungen ihrer Kinder, sondern für die Verletzung der eigenen Aufsichtspflicht haften)
- Allzuständigkeit verwandelt sich in allgemeine Aufsichtspflicht

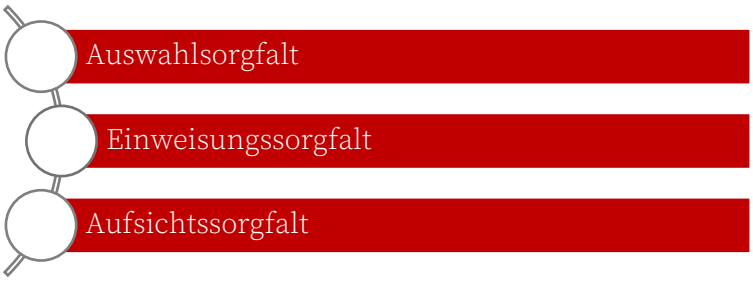
Daraus ergibt sich die Notwendigkeit, zwei Grundsätze beim Aufbau einer Compliance-Organisation miteinander zu kombinieren: den Vertrauensgrundsatz und die Misstrauensorganisation. Bei der Organisation des Unternehmens darf und sollte die Geschäftsleitung den Unternehmensangehörigen gegenüber genügend Vertrauen entgegenbringen, insbesondere hinsichtlich der Pflichterfüllung, der Kompetenzen und der Kenntnisse, allerdings ist diese Organisation so aufzubauen, dass ausreichende Mechanismen vorhanden sind, dies jederzeit zu kontrollieren und nötigenfalls einzugreifen, um Rechtsverstöße zu vermeiden (oder zumindest die Konsequenzen dieser zu minimieren).



Nicht delegierbar sind indes:

- Unmittelbar auferlegte Pflichten („der Vorstand hat…“)
- Genuine Aufgaben (Leitung der Gesellschaft, primäre Handlungspflichten wie Risikomanagement, Compliance, Unternehmensführung)

Bei der Delegation sind besonders drei Dimensionen der unternehmerischen Sorgfalt von Bedeutung:



Die **Auswahlsorgfalt** bedeutet besondere Aufmerksamkeit bei der Wahl geeigneter Unternehmensangehöriger. Die Funktionen, die einer Mitarbeiterin oder einem Mitarbeiter übertragen werden, sollten ihrem/seinem Profil, Bildung und Kenntnissen entsprechen, sie/er muss für die Aufgaben geeignet sein und den Umfang seiner Pflichten verstehen können.

Die **Einweisungssorgfalt** bedeutet die Notwendigkeit, jede:n Mitarbeiter:in in seine Aufgaben, in die interne Organisation, in die Abläufe im Unternehmen einzuweisen. Ob eine neue Persönlichkeit im Unternehmen oder jemand, wer von einer in eine andere Stelle „versetzt“ wird – jeder Mensch braucht Informationen bezüglich seiner konkreten Aufgaben, der Aufgabenerfüllung, der Berichterstattung etc. Das ist die Pflicht der Geschäftsleitung.

Die **Aufsichtssorgfalt** bedeutet schließlich die Pflicht der Geschäftsleitung, ordnungsgemäße Pflichterfüllung durch Unternehmensangehörige zu kontrollieren, um Pflichtverletzungen zu vermeiden. Es geht nicht um eine anlasslose Überwachung „auf Schritt und Tritt“, sondern vielmehr um Mechanismen und Prozesse, die die Überprüfung und Aufsicht über Pflichterfüllung möglich machen, wie etwa das Vier-Augen-Prinzip, Genehmigungsvorbehalte oder gemeinsame Entscheidungsfindung.

4.2.3 Business Judgement Rule

Die Business Judgement Rule bildet einen sogenannten „sicheren Hafen“: Sind die gesetzlichen Voraussetzungen dieser Regel erfüllt, ist die Geschäftsleitung von der Haftung für einen Schaden befreit. Die Business Judgement Rule sorgt für mehr Freiheit bei unternehmerischen Entscheidungen und lässt die Geschäftsleitung entspannter Entscheidungen treffen, die sich ggf. negativ auf das Unternehmen auswirken werden.

Gem. § 93 Abs. 1 S. 2 AktG: Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer **unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.**

Die gesetzlichen Voraussetzungen sind also:

- Unternehmerische Entscheidung

  Es handelt sich hierbei um eine nicht gebundene, also nicht bereits gesetzlich vorgeschriebene, Entscheidung: So kann der/die Geschäftsführer:in entscheiden, welche Software er/sie für die Führung eines datenschutzrechtlich notwendigen Verzeichnisses der Verarbeitungstätigkeiten einsetzen möchte, nicht aber, ob dieses Verzeichnis überhaupt geführt wird (es sei denn es liegt eine gesetzliche Ausnahme vor).

- Angemessene Information

  Diese Voraussetzung stellt jede Geschäftsleitung vor Herausforderungen, denn eine pauschale Bestimmung der Angemessenheit von geholten oder noch einzuholenden Informationen ist nicht möglich. Vielmehr hängt der Umfang der Informationen, die für eine Entscheidung notwendig sind, von der Art dieser Entscheidung und ihren möglichen Konsequenzen. So bedarf eine Entscheidung über eine einmalige Lieferung des Druckpapiers keine langen Informationsvorbereitung, eine Entscheidung über sicherheitsrelevante IT-Anbieter jedoch schon.

- Handeln zum Wohle der Gesellschaft

  Die Geschäftsleitung soll – wie ober bereits an einer anderen Stelle erwähnt – stets die Interessen des Unternehmens wahren und beim eigenen Handeln befolgen. Die getroffene Entscheidung muss also dem Wohle des Unternehmens dienen.

- Freiheit von Interessenkonflikten

  Schließlich ist es wichtig, dass die getroffene Entscheidung frei von Interessenskonflikten getroffen wird. Die Geschäftsleitung darf also lediglich das Interesse des Unternehmens verfolgen und nicht zusätzlich noch persönlich von der getroffenen Entscheidung oder ihren Konsequenzen und Folgen profitieren.

Liegen all diese Voraussetzungen vor – die natürlich nur einzelfallbezogen bestimmt werden können – kann der ggf. entstandene Schaden der Unternehmensleitung nicht „angelastet“ werden. Es kann ja immer passieren, dass eine vernünftige sorgfältig vorbereitete Entscheidung nicht zum gewünschten Ergebnis führt. Die Geschäftsleitung dafür haften zu lassen wäre unbillig und im Hinblick auf die Motivation und Mut zu Veränderungen hinderlich.

5 Compliance Organisation – Grundelemente

5.1 Überblick

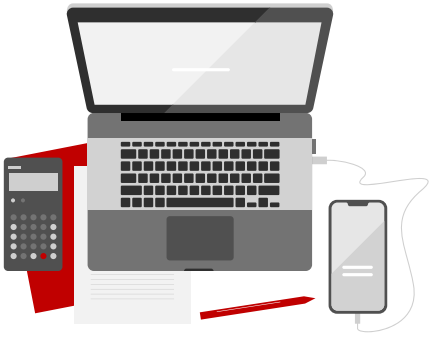
Zu einer wirksamen Compliance gehören:

- Risikoanalyse bzw. Risk Management
- Compliance-Kultur
- Compliance-Kommunikation
- Compliance-Organisation
- Überwachung

5.2 Risikomanagement

Risikomanagement ist die **Grundlage der Compliance-Organisation**, hängen doch die Maßnahmen, die Schulungen und auch die Kommunikation von den konkreten Risiken in jedem konkreten Unternehmen ab. Risikomanagement im Rahmen der Compliance ist jedoch kein eigenständiger Prozess, vielmehr müssen die Geschäftsprozesse „begleitet“ werden, mithin das Compliance-Risikomanagement eine gewisse „Support“-Rolle übernehmen. Empfehlenswert ist in dieser Hinsicht die Verbindung zweier Management-Taktiken für die besten Ergebnisse: einerseits die Top-Down-Technik, bei der die Geschäftsleitung „die erste Geige“ spielt, und andererseits die „Bottom-Up-Technik“, bei der die Beschäftigten aus ihrer Perspektive berichten. So werden die möglichen Risiken bestmöglich abgedeckt, denn die Geschäftsleitung hat einen Überblick über das gesamte Unternehmen, die Beschäftigten kennen ihre Prozesse und die diesen innewohnenden Risiken besser als jeder externe Beratende. Vorhandene Strukturen, Prozesse oder auch Risikokataloge unterstützen das Unternehmen bei der Ermittlung seiner Risiken.

Sind die Risiken einmal identifiziert, müssen sie bewertet, strukturiert und klassifiziert werden. Gerade bei der Bewertung von Risiken helfen – neben den notwendigen internen Kenntnissen und allgemeinen wirtschaftspolitischen Überlegungen – solche Tabellen wie hier dargestellt:



Eintritts-wahrschein-lichkeit / Risiko-bedeutung	Nicht bis kaum vorstellbar	unwahrscheinlich	Ggf. plausibel	wahrscheinlich	unvermeidbar
vernachlässigbar					
gering					
moderat / durchschnittlich					
bedeutend					
existenzvernichtend					

Grüne Farbe bedeutet dabei ein vernachlässigbares Risiko, gelbe – ein mittleres Risiko, rote – ein erstzunehmendes und dunkelrote sorgt für die höchste Alarmstufe.

Da gerade Compliance-Risiken teilweise schwer zu beziffern sind (etwa weil es um Rufschädigung gehen könnte), bietet sich bei der Bewertung eine Kombination aus finanziellen und nicht-finanziellen Bewertungskriterien an. Zu den nicht-finanziellen Bewertungskriterien könnten dann beispielsweise der Verlust mehrerer Leitungsangestellter wegen des sozialen Drucks, anhaltende Schwierigkeiten bei der Stellenbesetzung oder ständige Berichterstattung in der Presse zählen.

Nach der Risikobewertung muss das Unternehmen entscheiden, welchen Risiken wie zu begegnen ist. Einige Risiken können getragen werden, andere werden etwa auf die Versicherungsunternehmen übertragen, andere werden eventuell zunächst einfach beobachtet. Für die größte Gruppe werden jedoch Maßnahmen erforderlich sein, die dabei helfen diese Risiken zu minimieren. Auch der Umfang dieser Maßnahmen sollte mit den Unternehmensangehörigen im Dialog bestimmt werden, denn sie sind diejenigen, die konkrete Maßnahmen vornehmen und in diesem Sinne auch „tragen“ müssen.

Wichtig ist es, das Risikomanagement als eine laufende Tätigkeit zu verstehen und die Risikoermittlung und -bewertung immer wieder neu durchzuführen. Das gesamte Unternehmensumfeld, inklusive Recht, Wirtschaft und Gesellschaft, verändert sich stetig, neue Risiken entstehen und alte Risiken verlieren an Bedeutung.

Ein gut aufgebautes Risikomanagement hilft dabei, keine Risiken zu übersehen und Verstöße zu vermeiden.

5.3 Compliance-Kultur

Idealerweise erfolgt die Befolgung der vorgeschriebenen Normen nicht aufgrund eines Befehls und vor dem Hintergrund der Angst vor Vergeltungs- oder Ahndungsmaßnahmen, sondern aus innerer Überzeugung. Somit ist die Unternehmenskultur, in der Regelverstöße inakzeptabel sind, ein bedeutender Hilfsmechanismus für die Compliance.

Was ist aber die Unternehmenskultur?

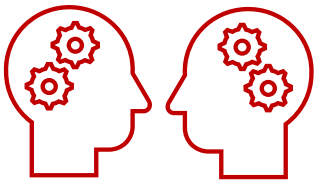
Es gibt viele Ansätze in vielen Wissenschaftszweigen, die Unternehmenskultur zu definieren:

Nach *Hofstede* etwa soll die gemeinsame Wahrnehmung der Praktiken in einem Unternehmen („shared perceptions of daily practices“) als eigentlicher Kern der Unternehmenskultur angesehen werden.

Nach *Schein* umfasst die Unternehmenskultur drei Ebenen:

- Grundannahmen sind dabei die Vorstellungen zu Beziehung zur Umwelt, Menschen, menschlichem Handeln, Wahrheit
- Normen und Standards – Richtlinien, Verbote, Werte (z.B. Leistung)
- Symbole – Architektur, Bekleidung, Bürogestaltung, Slang, Anekdote etc.

Nach *Luhmann* ist der zentrale Begriff der Unternehmenskultur die Kommunikation, die ihrerseits aus Information, Mitteilung und Verstehen besteht; demnach berührt die Unternehmenskultur die Identitätswahrnehmung der Mitarbeiter.



Unabhängig davon, welchen dieser Ansätze Sie am sympathischsten finden, scheinen alle sich zumindest darüber einig zu ein, dass die Unternehmenskultur das Management stärker kontrolliert als andersherum. Es ist also in erster Linie die Unternehmenskultur, die Manager:innen beeinflusst und es sind die Manager:innen, die die Unternehmenskultur bestimmen – hier sind die gegenseitigen Auswirkungen nicht von der Hand zu weisen.

Die Unternehmenskultur hat also eindeutig Auswirkungen auf die Compliance und ist beim Aufbau einer Compliance-Organisation von großer Bedeutung. Daher spricht man auch von der Compliance-Kultur als eine das regelkonforme Verhalten der Mitarbeiter fördernde Unternehmenskultur.

Die Wichtigkeit der Compliance-Kultur, ihre Bedeutung als „Herzstück der Compliance“ wird in vielen normativen Dokumenten; Empfehlungen und Richtlinien unterstrichen:

- Bundesanstalt für Finanzdienstleistungsaufsicht:

  „Im Kern zielen die neuen Anforderungen an die Compliance-Funktion auf eine **angemessene Compliance-Kultur**…“

- Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer:

  Compliance-Kultur als Kern des CMS

- ISO 37301:2021 Compliance Management System:

  „Compliance culture: the values, ethics and beliefs that exist throughout an organization … to produce **behavioral norms that are conducive to compliance** outcomes.“

- U.S. DoJ/U.S. SEC: A Resource Guide to the U.S. Foreign Corrupt Practices Act:

  “An effective compliance program promotes an organizational culture that encourages ethical conduct and a commitment to compliance with the law”

  “A strong ethical culture directly supports a strong compliance program.”

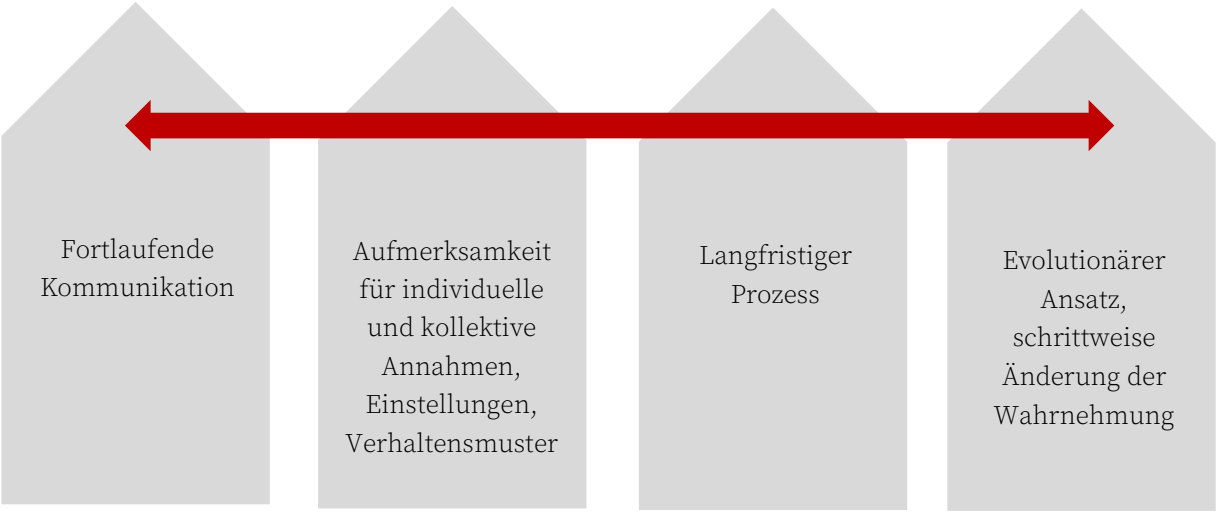
- U.S. Sentencing Commission: Federal Sentencing Guidelines Manual:

  „an organization shall … promote an organizational **culture that encourages ethical conduct and a commitment to compliance with the law**”

- Ministry of Justice, UK: Guidance UK Bribery Act:

  „…foster a culture within the organization in which bribery is never acceptable”

Um diesen Anforderungen Gerecht zu werden, muss die Etablierung der Compliance-Kultur auf folgende **vier Säulen** aufbauen:



Die Compliance-Kultur ist – genauso wie jede andere Kultur – leider nicht „per Dekret“ etablierbar und es ist unmöglich, mithilfe von internen Dokumenten die Compliance-Kultur „ein für alle Mal“ aufzubauen. Dieser langwierige schrittweise Prozess nimmt seine Zeit und Ressourcen in Anspruch, belohnt aber, richtig gestaltet, mit der Unternehmenskultur, in der Regelverstöße „von Hause aus“ vermieden werden.

Der Aufbau der Compliance-Kultur erfolgt über solche Techniken wie Tone at the Top und Tone from the Top:

Das Management ist sich des Themas Compliance bewusst, adressiert das Thema und hebt seine Bedeutung für die Belegschaft hervor sowie dient als Vorbild. Übt etwa das Management den Leistungsdruck aus und stellt unseriöse Praktiken nicht in Frage, kann es nicht von den übrigen Unternehmensangehörigen erwarten, dass sie sich der Compliance innerlich verpflichten und keine Abweichung vom Gesetz, internen Richtlinien und ethischen Grundsätzen zulassen.

Hilfreich für die Bestimmung dessen, was im Unternehmen wie gelebt wird, ist der sogenannte Code of Conduct oder Verhaltenskodex. Dort werden die wichtigsten Verhaltensgrundsätze formuliert und den Beschäftigten erklärt. Der Code of Conduct und seine Grundsätze sollten jedoch „gelebt“ werden – auf dem Papier festgehaltene Regeln, die im Unternehmen auf Ablehnung stoßen und nicht umgesetzt werden, bringen der Compliance keinen Zugewinn.

Als Richtschnur könnte das Unternehmen beispielsweise das sogenannte Null-Toleranz-Prinzip etablieren: Kein Compliance-Verstoß wird demnach im Unternehmen toleriert. Das soll nicht dazu verleiten, Menschen, die einen Fehler gemacht haben, sofort zu entlassen und schadensersatzpflichtig zu machen. Es soll vielmehr dem Verständnis dienen, dass wirklich jede Rechtsverletzung aufzudecken ist, zu ahnden (ggf. auch einfach mit einem Gespräch oder dem Entzug bestimmter Funktionen oder Kompetenzen) und – und das ist besonders wichtig – das Unternehmen und seine Prozesse daraufhin so anzupassen, dass eine erneute Rechtsverletzung entweder gänzlich unmöglich oder zumindest wesentlich erschwert wird.

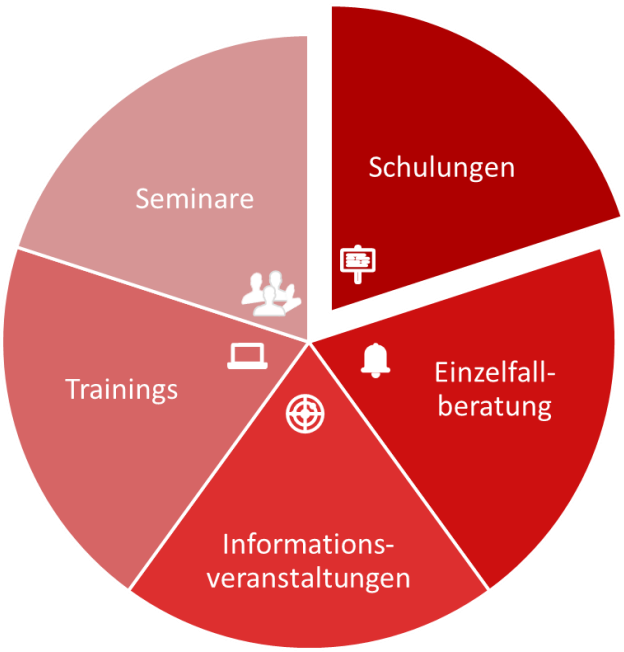
Null-Toleranz-Prinzip

- In den Verhaltensgrundsätzen verankern
- Einführung eines Hinweisgebersystems überlegen
- Mitarbeiter sollen ermutigt werden, Fehlverhalten zu melden
- Jeder Hinweis soll verfolgt werden
- Jedes Fehlverhalten soll geahndet werden
- Vorsicht bei der Schaffung des Misstrauensklimas (Stichwort: Denunziation)

5.4 Compliance-Kommunikation

Die Compliance will und muss den Unternehmensangehörigen kommuniziert werden. Es geht dabei um:

- Informationsbereitstellung
- Schulungen, Trainings, Seminare etc.
- Sensibilisierung/allgemeine Beratung
- Einzelfallbezogene Beratung
- Hinweisgebersysteme



Informationen mit Bezug zur Compliance – sei es der Code of Conduct oder die Entscheidungsfindungsleitlinien oder Informationsbeschaffungskriterien – müssen durch die Unternehmensleitung so zur Verfügung gestellt werden, dass sie auch abgerufen und verwendet werden können.

Es soll in Fragen der Compliance sowohl ganz allgemein – warum die Regeleinhaltung zwingend erforderlich, als auch bereichsbezogen – welche Regeln gelten etwa bei Vertragsabschluss in der Einkaufsabteilung, bei Informationsveranstaltungen und Schulungen – durchgeführt werden. Dabei ist darauf zu achten, dass die Beschäftigten nicht mit einer Unmenge an Informationen überfordert werden und „den Wald hinter den Bäumen“ nicht (mehr) erkennen können. In jedem Unternehmensbereich gibt es Besonderheiten, die eben nur in diesem Bereich eine Bedeutung haben – in der Personalabteilung spielt der Beschäftigtendatenschutz eine große Rolle, im Einkauf die Korruptionsprävention, im Vertrieb das Wettbewerbsrecht. Auf diese soll also auch präzise eingegangen werden, und teilweise werden das die Abteilungen selbst sogar besser einschätzen können als externe Berater oder die Geschäftsleitung. Wichtig ist dabei, genügend Vertrauen entgegenzubringen und doch auf die Rechtskonformität bestehender Praktiken zu achten.

Auch die einzelfallbezogene Beratung durch die Compliance-Stelle, durch die Rechtsabteilung oder durch die Geschäftsleitung sollte angeboten werden, denn teilweise liefern die allgemein gehaltenen Informationsveranstaltungen keine ausreichend präzisen Antworten.

Schließlich ist die Einführung von Hinweisgebersystemen zu bedenken: Diese können einen enormen Wert für die Aufdeckung von Rechtsverstößen bieten, bergen aber auch die Gefahr der Denunziation, wie oben bereits erwähnt. Eine individuelle, auf den Gegebenheiten des konkreten Unternehmens aufbauende Bewertung ist daher unerlässlich.

Was ist jedoch das **Wichtigste bei der Kommunikation**?

Die Kommunikation muss eindeutig sein, mit **klaren** verständlichen **Formulierungen**, in der Sprache, die in der Belegschaft gesprochen wird, auf dem Niveau, das an die konkreten Menschen angepasst ist. Sie muss die **gelebte** Unternehmenskultur und die angestrebte Compliance-Kultur wiedergeben und nicht so tun, als ob das Unternehmens komplett frei von jeglichem Fehlverhalten wäre. Sie muss die **Vorbildfunktion** der Führungskräfte befürworten, ihre Rolle bekräftigen, ihre Verantwortung unterstreichen. Sie muss **Integrität**, Vertrauen, Zuverlässigkeit als hohe Werte vermitteln, denn integre zuverlässige Menschen halten sich in aller Regel an das geltende Recht.

5.5 Compliance-Organisation

Die Compliance-Organisation im eigentlichen Sinne umfasst die Bildung einer Compliance-Stelle – sei es ein Compliance-Officer, Compliance-Manager, eine Compliance-Abteilung oder ein Compliance-Committee etc.

Diese Compliance-Stelle muss

- unabhängig
- kompetent
- mit notwendigen Ressourcen und Befugnissen ausgestattet
- durchsetzungsfähig

sein, um ihrer Funktion sinnvoll nachkommen zu können. Sie wird bei der Bestimmung und Einführung von Compliance-Prozessen (bspw. Vier-Augen-Prinzip) unterstützen, sie wird für klare Aufgabenverteilung im Unternehmen (sowohl bei compliance-spezifischen als auch bei allen anderen Funktionen) sorgen und einige Dokumentierungspflichten übernehmen müssen.

Dabei lässt sich die Compliance im engeren Sinne über zwei „Schutzgraben“ organisieren:

- Wahrnehmung der Compliance-Pflicht durch die Geschäftsleitung bildet dabei die sogenannte **First Line of Defense**
- Schaffung einer Compliance-Stelle sorgt dann für die sogenannte **Second Line of Defense**

Wie oben dargestellt, kann die Geschäftsleitung die Gesamtverantwortung für Compliance nicht durch Übertragung auf nachgeordnete Unternehmensebenen „loswerden“. Daher ist diese **First Line of Defense** zumindest genauso wichtig wie die eigentliche Compliance-Stelle.

Die Compliance-Stelle muss mit

- konkreten Aufgaben,
- klaren Befugnisse und Kompetenzen,
- angemessenen Ressourcen und
- klarer organisatorische Zuordnung

ausgestattet werden. Ihr müssen klare Berichterstattungswege gezeigt werden. Sie ihrerseits soll unbedingt – neben den gesetzlichen und wirtschaftlichen Vorgaben – die lokalen bzw. regionalen Besonderheiten berücksichtigen.

Die Compliance-Stelle muss nicht zwingend Rechtswissenschaften studiert haben; beim Berufsbild eines Compliance-Officers entdeckt man eine auffallende Vielfalt. Andererseits sind Rechtskenntnisse unabdingbar, sodass spätestens bei der Übertragung der Compliance-Funktion auf eine bestimmte Person zusätzliche Bildungskosten vom Unternehmen zu tragen sein werden.

Ein weiteres Element der Compliance-Organisation ist das Compliance-Programm. Es geht dabei sowohl um ein Compliance Management System als auch um Richtlinien und Kontrollmechanismen, die im Unternehmen etabliert werden müssen.

Folgende Grundsätze sind dabei zu beachten:

- Einhaltung in- und ausländischer Gesetze (Bestechung, § 299 StGB, Kartellverbot Art. 101 AEUV, § 1 GWB, Verbot unlauteren Wettbewerbs nach UWG, Gleichbehandlungsgrundsatz etc.)
- Unternehmensinterne Richtlinien (Regeln und Vorgehensweise, Handlungsanweisungen etc.)
- spezifische Compliance-Prozesse sowie Einbindung von Compliance in die bestehenden Geschäftsprozesse
- Kontrollsystem

Compliance-Programm ist als eine Karte wahrnehmbar, die bei der Suche nach den richtigen Antworten helfen soll. Es soll daher klar gestaltet sein, etwa nach den Maßstäben der ISO-Norm 37301:2021 oder des IDW-Standards 980, alle Bereiche des Unternehmens abdecken und stets am Laufen gehalten werden.

5.6 Überwachung

Das letzte Element einer Compliance ist die Überwachung. Wie oben bereits dargestellt, ist eine Unternehmensführung ohne Überwachung undenkbar, da der Gesetzgeber eine solche für notwendig hält und jedem Unternehmen(sträger) unmittelbar vorschreibt.

Worum geht es aber bei der Überwachung im Rahmen der Compliance-Organisation?

- Sowohl die Überwachung der Mitarbeiter:innen als auch die Überwachung der Compliance-Stelle/CMS/Compliance-Programms
- Prüfung der Compliance durch die interne Revision mindestens jährlich
- Bei einem Hinweis werden Untersuchungen eingeleitet (intern oder auch extern)
- Ergebnisse der Untersuchungen führen einerseits zur Ahndung der Schuldigen, andererseits müssen diese für die Verbesserung des vorhandenen Systems genutzt werden
- Kontrollrahmen muss verbindlich etabliert werden

Die Compliance-Organisation im engeren Sinne und die Überwachung zeigen Wechselwirkungen, denn Ergebnisse der Überwachung fließen in die Compliance-Organisation und helfen, diese zu verbessern, die Überwachung ist aber nur im Rahmen der Organisation (mitunter beim etablierten Kontrollrahmen) durchgeführt werden.

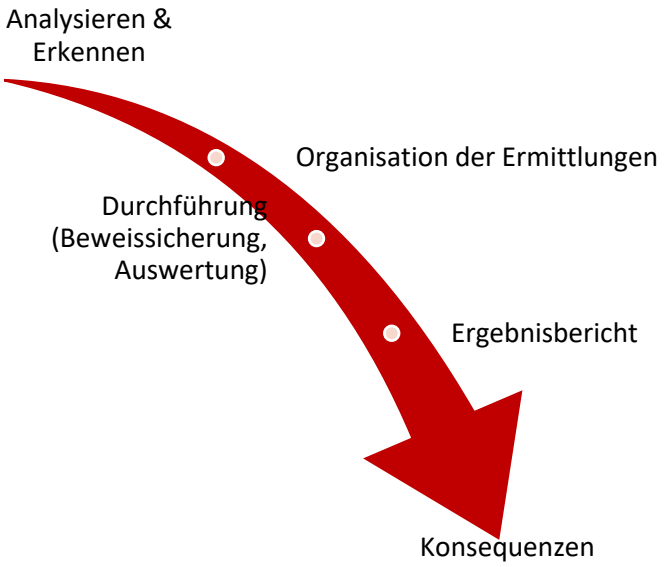
Eine wichtige Rolle in diesem Zusammenhang spielt die (falls vorhanden) Abteilung Internal Investigations.

Sie wird in aller Regel in der einen oder der anderen Form notwendig sein: auch wenn eine juristische Pflicht zur Aufklärung von Regelverstößen nicht besteht, ergibt sich eine faktische Pflicht zur Aufklärung. Dabei sind einzelne Maßnahmen und Verfahren nicht unproblematisch, geht es doch um

- Auswertung von Informationen,
- Befragungen der Mitarbeiter:innen (Teilnahme- und Auskunftspflicht),
- Whistleblowing,
- Verwendung der Informationen im eventuell folgenden Strafverfahren, sowie
- Beweissicherung.

Da sowohl Persönlichkeitsschutz und Datenschutz als auch speziellere gesetzliche Vorschriften (etwa zum Fernmeldegeheimnis) eine große Rolle spielen, dürfen diese rechtlichen Garantien nicht mit dem Verweis „das ist notwendig für die Aufklärung“ beiseitegeschoben werden. Dementsprechend ist stets darauf zu achten, dass auch die Compliance-Verfahren, u.a. auch die Aufklärung, selbst compliant, mithin regelkonform, sind.

Die Aufklärung dürfte allgemein dem folgenden Verlauf folgen:



Ermittelnde müssen sowohl fachlich als auch persönlich geeignet sein, diese recht schwierige Aufgabe zu übernehmen. Auch sie müssen in Bezug auf die Compliance geschult werden. Auch für sie gibt es bestimmte Grenzen, wie etwa strafgesetzlich bewährte Amtsanmaßung, § 132 StGB, oder Nötigung, § 240 StGB, datenschutzrechtliche Schranken oder Verletzung von Privatgeheimnissen.

6 Fazit

Wir haben uns zum Ziel gesetzt Ihnen zu zeigen, wie eine Compliance-Organisation in Ihrem Unternehmen aufgebaut werden könnte. Dabei haben wir sowohl einige Rechtsbereiche als auch die Besonderheiten Ihres Unternehmens unberücksichtigt gelassen. Trotzdem ist es uns hoffentlich gelungen, einen Überblick über die notwendigen Elemente einer jeden gut funktionierenden Compliance-Organisation – unabhängig von der Größe und der Branche Ihres Unternehmens – zu geben und die wichtigsten Themen in diesem Kontext anzusprechen. Compliance ist eines der zentralen Handlungsfelder eines jeden Unternehmens und trägt, wie aufgezeigt, zum nachhaltigen Bestand des Unternehmens in der Wirtschaftswirklichkeit. Natürlich können Verstöße gegen Regel und Pflicht nicht komplett ausgeräumt werden, das erwartet aber auch der Gesetzgeber nicht. Es geht bei der Compliance um eine vernünftig funktionierende Organisation des Unternehmens, die darauf gerichtet ist, dass anwendbare Normen von dem Unternehmen, also eigentlich von den Unternehmensangehörigen, da das Unternehmen selbst als solches nicht handlungsfähig ist, eingehalten und befolgt werden.

Die Schwierigkeiten des Wirtschaftens liegen unter anderem auch darin, dass sowohl das rechtliche als auch das wirtschaftspolitische Umfeld sich stetig verändert. Um diesen Änderungen nicht die Chance zu geben, dem Unternehmen zu schaden, empfiehlt sich eine ausgewogene und sich selbst ständig anpassende Compliance-Organisation. Dieser Leitfaden wird Sie hoffentlich dahingehend unterstützen, die Compliance-Organisation in Ihrem Unternehmen so zu gestalten, dass die meisten Risiken erkannt, bewertet und „abgedeckt“ sind und die Regeleinhaltung zum Teil Ihrer Unternehmenskultur, -strategie und -wahrnehmung geworden ist.

Wir wünschen Ihnen dabei viel Erfolg!

7 Kontakt

Wenn Sie Fragen oder Anregungen zu diesem Leitfaden haben, lassen Sie es uns wissen. Wir stehen Ihnen gerne zur Verfügung.

Olga Kunkel, LL.M., zert. DSB nach EU-DSGVO

Telefon: +49 3375 508 641

Email: olga.kunkel@itwirtschaft.de

Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft

Schiffbauerdamm 40

10117 Berlin

www.itwirtschaft.de

Was ist Mittelstand-Digital?

Das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft ist Teil der Förderinitiative Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter: www.mittelstand-digital.de

Stand: Oktober 2022