Ingrid Wiedemann
Patrick Pobuda

Compliance in der Forschung

Praxisnahes Grundwissen von der Risikoanalyse über effektive Präventionsmaßnahmen zu einem wirksamen System

Springer Gabler

Compliance in der Forschung

Ingrid Wiedemann • Patrick Pobuda

Compliance in der Forschung

Praxisnahes Grundwissen von der Risikoanalyse über effektive Präventionsmaßnahmen zu einem wirksamen System

Springer Gabler

Ingrid Wiedemann
Fraunhofer-Gesellschaft
München, Deutschland

Patrick Pobuda
Fraunhofer-Gesellschaft
München, Deutschland

ISBN 978-3-658-45727-3 ISBN 978-3-658-45728-0 (eBook)
https://doi.org/10.1007/978-3-658-45728-0

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Dieses einführende Werk in die Welt der Compliance ist im Rahmen unserer beruflichen Tätigkeit in der Zentrale der Fraunhofer-Gesellschaft in München entstanden. Es soll hiermit ein unkomplizierter sowie auch schneller Einstieg in dieses spannende Themenfeld gelingen. Vor allem wird die Compliance-Arbeit in Forschung und Wissenschaft adressiert. Die ersten beiden Kapitel befassen sich mit den grundlegenden Aspekten, die Kapitel drei bis sechs stellen die jeweiligen Bestandteile des hier umrissenen Compliance-Kreislaufes – im Sinne eines simplen Vorgehensmodells – dar, Kapitel sieben behandelt verschiedene relevante Einzelthemen und Kapitel acht bildet den Abschluss mit einem Resümee sowie Ausblick auf zukünftige Herausforderungen. Jedes Kapitel enthält zudem Empfehlungen für weiterführende Literatur zum jeweiligen Themenbereich. Ferner wurde versucht, neben allgemein-anerkannten Inhalten ebenso unsere Erfahrungen aus der Compliance-Tätigkeit in einer außeruniversitären Forschungseinrichtung einzubringen. Dennoch ist hiermit keine Best-Practice-Anleitung angestrebt, sondern lediglich eine initiale Hilfestellung, um recht zügig den Kern der Compliance und auch ihre Aufgaben verstehen zu können.

Natürlich ist dieses Buch nicht nur in einer isolierten Arbeitsgemeinschaft bestehend aus zwei Personen entstanden – wobei die Erstellung durch die beiden Autor:innen zu gleichen Teilen erfolgte. Vielmehr ist es durch einen lebhaften Austausch zwischen verschiedenen Menschen gewachsen. Deshalb möchten wir uns herzlichst bei unseren Kolleg:innen in der Fraunhofer-Gesellschaft, insbesondere bei Dr. Markus Zirkel und Dr. Anne Funck Hansen, für ihre Unterstützung im Rahmen dieser Bucherstellung bedanken. Ebenso gilt unser tiefer Dank den Expert:innen Markus Jüttner und Dr. Hubert Schmid wie auch Anna Schmid und Julia Wiedemann, die uns in ihrem jeweiligen Fachbereich mit wertvollen Hinweisen/Kommentaren sehr weitergeholfen haben.

An dieser Stelle soll ferner darauf hingewiesen werden, dass die in diesem Buch vorgestellten Vorgehensweisen, Konzepte und Empfehlungen lediglich die Sichtweise der beiden Autor:innen abbilden sowie nicht im Gesamtkontext der Fraunhofer-Gesellschaft zu verstehen sind. Es handelt sich hierbei also weder um eine etwaige Beschreibung bzw. Darstellung des Compliance-Management-Systems oder der Compliance-Organisation von Fraunhofer noch sollen hiermit in irgendeiner Weise mögliche Andeutungen oder eventuelle Bewertungen aufgezeigt bzw. offenbart werden.

Wir hoffen, dass unsere Intention, mit diesem Buch eine nützliche Hilfestellung zum Einstieg in die Compliance-Arbeit für Forschung und Wissenschaft bereitstellen zu können, auch wirklich gelungen ist, und wünschen Ihnen viel Erfolg bei der individuellen sowie herausfordernden Aufgabenstellung, die Compliance in Ihrer jeweiligen Organisation wirksam voranzubringen.

München, Deutschland

Ingrid Wiedemann
Patrick Pobuda

Über dieses Buch

Was Sie in diesem Buch finden können

- Einen ersten Überblick zu den wesentlichen Compliance-Grundlagen im Allgemeinen sowie eine tiefere Hinführung zu den Compliance-Gegebenheiten in der Wissenschaft.
- Eine geordnete bzw. strukturierte Vorgehensweise, mit der eine agile Implementierung und ein nachhaltiger Betrieb eines Compliance-Management-Systems gelingen kann.
- Einen Einblick in die notwendigen Fähigkeiten für eine erfolgreiche Compliance-Arbeit mit einem Plädoyer für eine organisationsweite Strategie inklusive Ziele für Compliance.
- Eine Hinführung zu den wesentlichsten etablierten Standards und relevanter Literatur sowie zu weiteren Informationsquellen und einschlägigen Verbänden der Compliance.
- Ein Darstellungsversuch des Enabling-Ansatzes, mit dem Compliance eben nicht als Belastung der Organisation, sondern als Chance zur Fortentwicklung verstanden wird.

Zusammenfassung

Dieses Buch beschäftigt sich mit dem Aufbau, wesentlichen Elementen sowie Wirksamkeitsmechanismen eines Compliance-Management-Systems in Forschung und Wissenschaft. Als ein zentrales Anliegen gilt es hier, einen Eindruck zu vermitteln, wie die Balance zwischen gesetzlichen sowie gesellschaftlichen Anforderungen und dem für Innovationen nötigen Freiräumen gelingen kann. Wo Grenzen sinnvoll gesetzt werden können und wie dies dann auch im Arbeitsalltag praktisch – bspw. durch das Einbringen von Leitplanken oder zielgruppenspezifischen Orientierungshilfen – realisiert werden kann, wird weithin verständ-

lich aufgezeigt. Es soll Personen mit unterschiedlichem Kenntnisstand – von Einsteiger:innen bis Fortgeschrittenen – entsprechende Perspektiven eröffnen, eine brauchbare Vorgehensweise aufzeigen sowie Wegweiser und nützliches Arbeitsmittel sein, um in der täglichen Compliance-Arbeit individuelle Lösungen erarbeiten zu können. Neben dem aktuellen Literaturstand zum Thema Compliance sind die praktischen Erfahrungen der beiden Autor:innen eingeflossen. Ferner wird in jedem Kapitel auf weiterführende Literatur verwiesen. Die Sammlung anwendungsorientierter Standards sowie realitätsnaher Beispiele soll den Lesenden die Implementierung erleichtern und einen Einblick in den Arbeitsalltag geben, wie die Konzepte usw. zu verstehen sind, welche dann spezifisch an die jeweiligen Gegebenheiten der Organisation anzupassen sind. Entsprechend wird hier ein möglichst breites Spektrum in Bezug auf die Organisationsdiversität im Umfeld von Wissenschaft und Forschung (z. B. Universität, Hochschule, außeruniversitäre Forschungseinrichtung sowie Wirtschaftsunternehmen) berücksichtigt. Allen ist jeweils die Notwendigkeit gemeinsam, ihre Innovationsfähigkeit zu stärken – um im Wettbewerb bestehen zu können – und die hierfür erforderlichen Handlungsmöglichkeiten zu schaffen, ohne dass dabei die sinnhaften Absichten hinter den gesetzlichen Vorgaben oder ethischen Standards etc. ausgehöhlt bzw. untergraben werden. Die Aspekte des Spannungsfelds zwischen Freiheit bzw. Gestaltungsspielräumen der Wissenschaft sowie Begrenzung durch verbindliche Bestimmungen werden in den hier verfolgten Ansätzen des *Enablings* bzw. *Möglichmachens* und *risikoorientierten Handelns* in den Vordergrund gestellt. Geleitet wird diese Vorgehensweise vom übergeordneten Ziel, die Compliance als starken Beitrag zum Organisationserfolg zu positionieren. Denn Compliance soll nicht durch eine Regelflut belasten, sondern durch kluge Maßnahmen rechtliche Sicherheit gewähren. So macht dieses Buch hoffentlich Lust auf die Compliance-Arbeit, ohne dabei jedoch die damit einhergehenden Anstrengungen bzw. Schwierigkeiten in der Umsetzung zu verschweigen.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
AKV	Aufgaben, Kompetenzen und Verantwortlichkeiten
AWR	Außenwirtschaftsrecht
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BCM	Bundesverband der Compliance-Manager
BDI	Bundesverband der Deutschen Industrie
BKA	Bundeskriminalamt
BMAS	Bundesministerium für Arbeit und Soziales
BMI	Bundesministerium des Innern und für Heimat
CCO	Chief Compliance Officer
CG	Corporate Governance
CMS	Compliance-Management-System
CoC	Code of Conduct
CPI	Corruption Perceptions Index
CPL	Compliance
CRM	Customer-Relationship-Management
CSDDD	Corporate Sustainability Due Diligence Directive
CSR	Corporate Social Responsibility
CSRD	Corporate Sustainability Reporting Directive
DCGK	Deutscher Corporate Governance Kodex
DICO	Deutsches Institut für Compliance
DOJ	US Department of Justice
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
ERP	Enterprise Resource Planning
ESG	Environmental Social Governance
EU	Europäische Union

EuGH	Europäischer Gerichtshof
FAQ	Frequently Asked Questions
F&E	Forschung und Entwicklung
FCPA	Foreign Corrupt Practices Act
GewO	Gewerbeordnung
GRC	Governance, Risk und Compliance
HinSchG	Hinweisgeberschutzgesetz
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IIA	Institute of Internal Auditors
IK	Interessenkonflikt
IKS	Internes Kontrollsystem
IP	Intellectual Property
KI	Künstliche Intelligenz
KPI	Key Performance Indicators
KVP	Kontinuierlicher Verbesserungsprozess
LkSG	Lieferkettensorgfaltspflichtengesetz
LobbyRG	Lobbyregistergesetz
NGO	Non-Governmental Organization
OECD	Organization for Economic Co-operation and Development
OwiG	Gesetz über Ordnungswidrigkeiten
PCDK	Public Corporate Governance Kodex
PS	Prüfungsstandard
QM	Qualitätsmanagement
StGB	Strafgesetzbuch
UK	United Kingdom
UKBA	United Kingdom Bribery Act
UN	United Nations
US	United States
VDA	Verband der Automobilindustrie

Abbildungsverzeichnis

Bedeutung/Nutzen der Compliance

1

Noch bis gut in die 1990er-Jahre galt in der Unternehmenswelt der Ansatz des einflussreichen Ökonomen Milton Friedman (1970), dem zufolge „the social responsibility of business is to increase its profits." Zum Glück hat für unserer aller Lebensqualität ein Umdenken stattgefunden, welches Unternehmen bzw. Organisationen – zunehmend – dazu verpflichtet, aus diesem engen Fokus auszubrechen und bspw. neben den Gesetzen zur Bekämpfung von Korruption oder der Durchsetzung des Außenwirtschaftsrechts ebenso Themenkomplexe wie Fairness, Menschenrechte und Umweltschutz stärker anzugehen (siehe in diesem Kontext die Konzepte *CSR – Corporate Social Responsibility* sowie *ESG – Environmental, Social and Governance*, welche sich derzeit sehr dynamisch entwickeln und eine fortschreitende Verrechtlichung erfahren). Getrieben wurde dieser Wandel bspw. durch die Einsicht, dass sich an den bis dato betriebenen Praktiken dringend etwas ändern muss, damit die Erde auch noch den nachfolgenden Generationen zur Verfügung steht, oder dass sich Gerechtigkeit auf breiter Ebene nicht mit warmen Worten erreichen lässt. Vor allem aber haben wohl geopolitische sowie wirtschaftliche Beweggründe dazu beigetragen, dass u. a. die Entwicklung des Globalen Südens eine höhere Priorität bekommen hat (z. B. Reduzierung der Migrationsströme) und dass mit natürlichen Ressourcen (z. B. infolge von Verknappung und somit Preissteigerungen) in nachhaltigerer (z. B. durch umfassendes Recycling) sowie sparsamerer Weise (u. a. mithilfe effizienter Produktionsverfahren) umgegangen wird. Selbst das Streben nach Fairness kann aus wirtschaftlichen Gründen erfolgen, denn ein anständiges Miteinander in einer Entität und darüber hinaus befördert die Performance bzw. steigert die Leistungsfähigkeit (z. B. treiben Chancengleichheit sowie Gleichberechtigung massiv das Engagement wie auch die Innovationsfähigkeit der Organisationsangehörigen). Ferner bildet natürlich

I. Wiedemann, P. Pobuda, *Compliance in der Forschung*,
https://doi.org/10.1007/978-3-658-45728-0_1

das Vertrauen bspw. der Investor:innen, Projektpartner:innen oder Kund:innen sowie Mitarbeitenden in die jeweiligen Tätigkeiten/Ziele einer Organisation die Grundlage für den (zweckorientierten bzw. wirtschaftlichen) Erfolg, wodurch u. a. die Einhaltung von Gesetzen oder der Schutz der eigenen Reputation essenziell ist. Ebenso zahlen diese Punkte sicherlich auf die Arbeitgeberattraktivität ein, was in Zeiten des Fachkräftemangels von erheblicher Wichtigkeit ist. Zweifelslos trugen auch die vielen gesellschaftlichen Initiativen und Protestbewegungen sowie sich daraus ergebende politische Bestrebungen zu diesem wichtigen Umdenken bei. Entsprechend stark ist also die Regulatorik gestiegen, welche vermutlich in Zukunft aufgrund großer Entwicklungen/Herausforderungen (wie *Künstliche Intelligenz* oder *Klimakrise*) weiter zunehmen wird. Mit diesen starken Veränderungen hat auch die Compliance erheblich an Bedeutung gewonnen und das nicht nur in der Privatwirtschaft, sondern in nahezu allen Organisationsformen (Abb. 1.1).

Compliance bezeichnet im weitesten Sinne die (Beschäftigung mit der) Regelkonformität einer Organisation (wie z. B. Forschungseinrichtungen, Unternehmen oder ähnlichem). Hierunter kann allgemein gesehen die Einhaltung der anzuwendenden nationalen und internationalen Gesetze, etablierten Standards oder auch selbstgesetzten Verhaltensnormen (was man kurzgefasst unter dem Begriff *Vorgaben* subsumieren könnte) durch die Führungskräfte sowie Mitarbeitenden usw. verstanden werden. Die *Corporate Compliance* beinhaltet das unternehmerische Handeln zur Beachtung dieser Vorgaben, für welche sich die Leitung einer Organisation verantwortlich zeichnet. Es gilt in erster Linie die einschlägigen Gesetze eines Landes einzuhalten. Ferner ergibt sich hieraus der Umstand, dass je internationaler eine Organisation agiert, desto umfassendere Bestimmungen beachtet werden müssen. Ein weiterer bedeutender Aspekt ist, dass sich die nationale oder auch supranationale Regulatorik (z. B. durch die EU) in Bezug auf das unternehmerische Handeln immer erheblicher an Nachhaltigkeitsaspekten orientiert und damit ebenso auf eine Steigerung der Resilienz von Organisationen abzielt, um u. a. in Krisensituationen widerstandsfähiger zu sein. Darüber hinaus gilt es die branchenspezifischen Vorgaben entsprechend zu befolgen. Zunehmend werden auch *weiche Faktoren* wie Fairness, Integrität sowie Geschäftsethik in die Compliance-Arbeit einbezogen und die strategischen Überlegungen daran ausgerichtet.

Mithilfe der Compliance können in systematischer Weise die jeweils anzuwendenden Vorgaben genau identifiziert sowie effektive Maßnahmen weitestgehend effizient umgesetzt werden, sodass potenzielle Risiken aus der Nichteinhaltung dieser Vorgaben (z. B. Bußgelder, Freiheitsstrafen oder Reputationsschäden und damit die Gefahr, den Organisationszweck zu verwirken) minimiert bzw. mitigiert werden können. Allerdings ist ebenso die konträre Richtung zu meiden, in der Compliance durch ein zu striktes Durchgreifen bzw. einen überbordenden Ver-

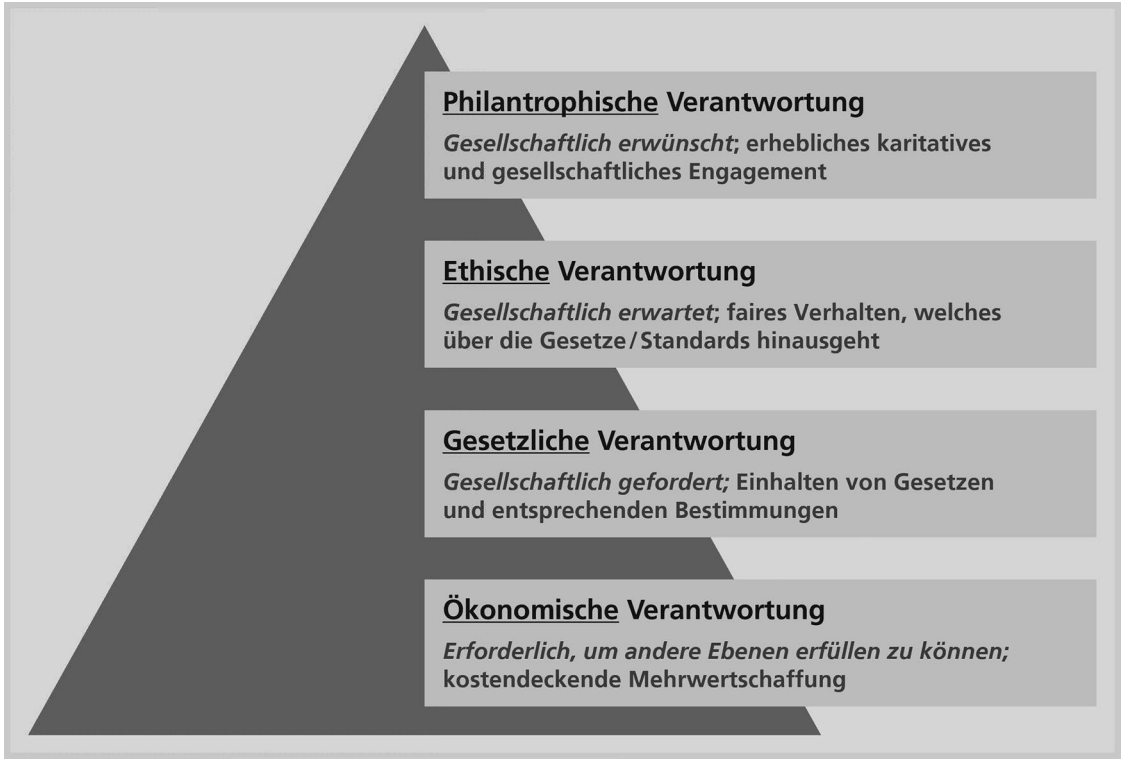

Abb. 1.1 Beziehung von Wirtschaft, Recht sowie CSR. (Vgl. Carroll 1991)

waltungsaufwand dafür sorgt, dass bspw. (wachsende) zusätzliche Kosten die Wirtschaftlichkeit gefährden. Prinzipiell sollte die Compliance somit eine Balance finden zwischen der Durchsetzung ihrer Anforderungen[1] bzw. gegebener Vorgaben (*Machtposition*) sowie ihrer Rolle als neutrale bzw. unterstützende Beraterin (*Vertrauensposition*). In diesem Sinne gilt es sich detailliert mit den jeweiligen Gesetzen etc. auseinanderzusetzen, nicht nur damit eine (rechtliche) Handlungssicherheit für die arbeitsbezogenen Aktivitäten der Entitätsangehörigen oder bspw. der Projektpartner:innen besteht, sondern auch damit einzelne organisationsspezifische Gestaltungsspielräume erkannt und entsprechend zweckdienlich ausgenutzt werden können (z. B. zur Schaffung von Freiräumen für Innovationen).

Gerade hinsichtlich Ausmaß bzw. Intensität der Compliance braucht es u. a. eine sinnvolle bzw. kluge[2] Abwägung zwischen harten Vorgaben wie auch Kontrollen und dem (durch eine unterstützende Unternehmenskultur verlässlich zu untermauernden) Vertrauen in das integere Verhalten der Mitarbeitenden bzw. Organisationsangehörigen sowie deren Führungskräften und dem Management. Denn bei einer (sehr) genauen Betrachtung wird man wohl bei jedem Menschen ein Fehlverhalten feststellen (ganz im Sinne des Ausspruchs, dass *unter der Lupe niemand gut aussieht*). Die grundsätzliche Frage aus Sicht der Organisationsleitung ist daher, welche Verstöße für die Organisation letztlich so schädlich sind, dass diesen jeweils entgegengewirkt werden muss bzw. welche Risiken so kritisch/relevant sind, dass diese (im Ramen der verfügbaren Mittel) angemessen und wirksam mitigiert werden müssen. Wesentlich schwieriger wird diese Abwägung noch dadurch, dass bereits eine einzelne Person in der Organisation durch individuelles – strafbares bzw. ethisch unkorrektes – Verhalten großen Schaden anrichten kann.

Entsprechend ist die Anwendung der Compliance zwangsläufig auch in Forschung sowie Wissenschaft essenziell, vor allem wenn es bspw. um den Transfer von Innovationen in die Wirtschaft geht oder im Kontext von Arbeitgeberattraktivität sowie als verlässliche/r Geschäfts- oder Projektpartner:in. Zudem sind im Bereich der wissenschaftlichen Arbeit bzw. Tätigkeit selbst natürlich reichlich Vorgaben einzuhalten, bspw. bei den Fragestellungen, mit welchen Datensätzen

[1] Eine Anforderung ist hier im Wesentlichen eine Aussage über die notwendige Eigenschaft oder Fähigkeit, welche zur Erreichung eines Zieles benötigt wird oder welche ein anvisiertes System (zwangsläufig auch) erfüllen muss bzw. sollte.

[2] Die Worte *sinnvoll* und *klug* werden in diesem Buch häufig verwendet und sollen dabei ausdrücken, dass u. a. in der Compliance-Arbeit infolge der diversen Gegebenheiten einer jeweiligen Organisation sowie deren Umfeld oftmals keine einfachen bzw. vorgefertigten Lösungen existieren können. Daher sind die Aufgaben bspw. mit gewissenhafter Konzentration sowie kreativer Cleverness anzugehen, ohne dass dabei der Zweck bzw. die Wirtschaftlichkeit etc. und damit der Organisationsnutzen konterkariert wird.

eine Künstliche Intelligenz jeweils trainiert werden darf (Stichwort *Datenschutz*) oder inwieweit Menschenaffen für medizinische Versuche bzw. Zwecke heranziehbar sind (Stichwort *Ethik*). In diesem Kontext gilt es auch sicherzustellen, dass dem wissenschaftlichen bzw. wirtschaftlichen Erfolg eben nicht ethische, gesetzliche oder organisationsspezifische Vorgaben geopfert werden. Es muss darüber hinaus zwingend vermieden werden, dass sich bspw. in der Organisation aufkeimendes negatives Verhalten (z. B. Zahlung von Bestechungsgeldern zur Auftragserlangung oder Inkaufnahme von Gesundheitsschäden beim Medikamententest) verstärken kann, wodurch sich Mitarbeitende diesem schädlichen Verhalten bzw. dieser Unternehmens-/Organisationskultur nicht entziehen (außer durch Kündigung) sowie ihre Karriere nicht mehr integer voranbringen können.

Damit nun Forschungseinrichtungen am Markt erfolgreich agieren können (um z. B. ihre Dienstleistungen im Bereich der angewandten Wissenschaften zu vertreiben oder auch innovative Geschäftsideen bzw. -modelle auf der Basis spannender Forschungsergebnisse durch Ausgründungen bzw. Startups zu verwirklichen), müssen sie sich den äußerst vielfältigen Anforderungen bzw. Erwartungen[3] stellen, die u. a. von den Behörden, der Zivilgesellschaft oder ebenso von Partner:innen an sie gerichtet werden. Im Kontext von Geschäfts- bzw. Kooperationspartnerschaften können Anforderungen bspw. Pflichten in Form von höheren, über Gesetze hinausgehende, Sozialstandards sein (wie z. B. die fakultative Zahlung des deutschen Mindestlohnes in den Niedriglohnländern des Globalen Südens). Durch das Festhalten solcher zusätzlichen Verpflichtungen in einer Eigenerklärung oder einem Verhaltenskodex (im Englischen als *Code of Conduct* bezeichnet) und deren Aufnahme in den jeweiligen Kooperationsvertrag etc. (wodurch ein Verhaltenskodex dann auch Vertragsbestandteil würde) gilt es diese verbindlich einzuhalten. Somit ergeben sich aus der Nichteinhaltung dieser (freiwilligen) Verpflichtungen entsprechende Ansprüche der Partner:innen (also z. B. Schadensersatzansprüche oder Vertragsstrafen). Damit das nicht geschieht und damit natürlich ebenso keine Strafen oder Reputationsschäden aufgrund von Verstößen gegen andere Vorgaben entstehen, müssen u. a. die sich aus Gesetzen ergebenden Anforderungen (z. B. arbeitsrechtliche Bestimmungen zum Gesundheitsschutz, wie die Installation von Absperrungen und Schutznetzen, oder die obligatorischen Grundsätze in

[3] Diese Erwartungen sind nicht nur divers, sondern häufig widersprüchlich. Denn Organisationen sollen zugleich Gesetze einhalten, die Umwelt schützen, Lieferketten im Blick haben, innovative Forschung betreiben und auch ein:e attraktive:r Arbeitgeber:in sein (neben weiteren Erwartungshaltungen). Daher lässt sich Compliance als das Verhalten einer Organisation auffassen, welches die Erwartungen externer Interessensgruppen erfüllt oder mit diesen möglichst übereinstimmt; vgl. Jüttner und Schütz (2023).

der Buchführung, wie die Aufbewahrungspflicht von Buchungsbelegen) unbedingt eingehalten werden. Demgemäß sollten Organisationen also stets in Einklang mit den jeweiligen (rechtlichen, ethischen etc.) Vorgaben agieren, da sich anderweitiges (gesetzeswidriges) Verhalten oftmals sehr schnell existenzbedrohend auf die allerbeste Geschäftsidee bzw. Innovation auswirken kann.

Infolge der ganzheitlichen Betrachtung aller – für die jeweilige Organisation anzuwendenden – Rechtsgebiete und selbstgesetzten Verpflichtungen sowie der sich daraus ergebenden Aktivitäten wird von einem (Management-)System[4] gesprochen. Das Compliance-Management-System (CMS) begründet sich auf einem organisationsspezifischen Risikomanagement mit u. a. turnusmäßig stattfindenden Risikoanalysen. Hiermit sind in einer Regelmäßigkeit (oder ggf. zusätzlich auch anlassbezogen) die gesetzlichen Vorgaben sowie damit verbundene haftungsrelevante oder (darüber hinausgehende) reputationsschädigende Risiken individuell für die jeweilige Entität zu erfassen. Davon abgeleitet sind Präventionsmaßnahmen zu erarbeiten, um diesen Risiken in effektiver und effizienter Weise entgegenwirken zu können. Sollten diese individuell zu konzipierenden Maßnahmen in der realen (Arbeits-)Welt dann doch mal zu kurz greifen, so müssen passende Abhilfemaßnahmen anberaumt werden, welche den entstandenen Schaden u. a. eingrenzen können. Ob nun die Präventionsmaßnahmen tatsächlich wirksam sind, ist über jeweilige Kontrollen aktiv zu überprüfen; ferner weisen ggf. Meldungen über das Hinweisgebersystem auf Systemmängel sowie Verstöße hin. Auch eine aussagekräftige Dokumentation für die Nachvollziehbarkeit der Compliance-Arbeit (z. B. als Argument für Gerichtsverfahren) und zielführende Berichterstattung an die notwendigen Funktionen bzw. Stellen (z. B. Organisationsleitung) über all diese verschiedenen Aktivitäten sind als Bestandteile eines CMS anzusehen. So bildet sich aus dieser umrissenen Systematik ein Kreislauf bzw. Regelkreis, der kontinuierlich abzulaufen hat. Letztendlich sollen also mit einem CMS die folgen-

[4] Unter dem Begriff *Managementsystem* versteht man im Allgemeinen das Folgende: „A management system is the way in which an organization manages the interrelated parts of its business in order to achieve its objectives. These objectives can relate to a number of different topics, including product or service quality, operational efficiency, environmental performance, health and safety in the workplace and many more. The level of complexity of the system will depend on each organization's specific context. For some organizations, especially smaller ones, it may simply mean having strong leadership from the business owner, providing a clear definition of what is expected from each individual employee and how they contribute to the organization's overall objectives, without the need for extensive documentation. More complex businesses operating, for example, in highly regulated sectors, may need extensive documentation and controls in order to fulfil their legal obligations and meet their organizational objectives." (ISO 2024).