

# 04.19

# ZRFC

14. Jahrgang  
August 2019  
Seiten 145–192

## Risk, Fraud & Compliance

[www.ZRFCdigital.de](http://www.ZRFCdigital.de)

### Herausgeber:

School of Governance, Risk &  
Compliance – Steinbeis-Hochschule  
Berlin

### Herausgeberbeirat:

Prof. Dr. Dr. habil. Wolfgang Becker,  
Otto-Friedrich-Universität Bamberg

RA Dr. Karl-Heinz Belser,  
Dépre Rechtsanwalts AG

RA Dr. Christian F. Bosse,  
Partner, Ernst & Young Law GmbH

Verena Brandt,  
Partner, KPMG AG

Prof. Dr. Kai-D. Bussmann,  
Martin-Luther-Universität  
Halle-Wittenberg

RA Bernd H. Klose, German Chapter of  
Association of Certified Fraud  
Examiners (ACFE) e. V.

RA Dr. Rainer Markfort,  
Partner, Dentons Europe LLP

Prof. Dr. Volker H. Peemöller,  
Friedrich-Alexander-Universität  
Erlangen-Nürnberg

RA Christian Rosinus,  
Wirtschaftsstrafrechtliche  
Vereinigung e. V., Vorstand

RA Prof. Dr. Monika Roth,  
Leiterin DAS Compliance Management,  
Hochschule Luzern

RA Raimund Röhrich,  
Lehrbeauftragter der School of  
Governance, Risk & Compliance

## Prävention und Aufdeckung durch Compliance-Organisationen

**Management** **Compliance in Hochschulen**  
Weber/Lejeune, 151

**Prevention** **Gestaltungsvorgaben für Hinweisgeber-  
systeme unter Berücksichtigung der  
Hinweisgebergefährdung**  
Behringer/Scherbarth, 157

**Detection** **Ermittlung einer Schadens-  
erwartungsgröße**  
Sure/Deckers, 166

**Legal** **Das GeschGeh-Compliance-  
Management-System**  
Schefold, 171  
**Wie sehen Unternehmen die Justiz?**  
Behringer/Passarge/Scherbarth/Unruh, 178

**Profession** **Compliance bewegt ...**  
Interview mit Christian Parsow, 187

**ESV** ERICH  
SCHMIDT  
VERLAG

In Kooperation mit  
**DICO**  
Deutsches Institut für Compliance

# Das GeschGeh-Compliance-Management-System

## Ein CMS zur erfolgreichen Verwertung eigener und zum Schutz vor Inanspruchnahme aus fremden Geschäftsgeheimnissen (GeschGehs)

Dr. Christian Schefold\*

*Das neue Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), welches im Zuge der verspäteten Umsetzung der Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung am 18. April 2019 erlassen wurde, wird den Umgang mit Know-how in Unternehmen deutlich verändern. Während früher Vertraulichkeitsvereinbarungen mit hohen Vertragsstrafen einen Schutz von Unternehmensinformationen durch Drohung herbeizuführen versuchten und dabei eine gerichtliche Durchsetzung oft schon an der Darlegung der Informationen und ihres Schutzgehaltes selbst scheiterte, gibt nun das GeschGehG Unternehmen Anhaltspunkte, um den Schutz von Geschäftsgeheimnissen aktiv zu gestalten. Das neue Gesetz setzt implizit die Compliance-Entwicklungen der letzten Jahre bis hin zur EU Datenschutzgrundverordnung (DSGVO) voraus, baut darauf auf und führt zusätzlich noch verfahrensrechtliche Regeln zum Informationsschutz ein. Dabei können Erfahrungen mit Compliance-Management-Systemen den Unternehmen helfen, die Chancen der Geschäftsgeheimnisse bestmöglich zu nutzen. Für Compliance bedeutet dies einen Paradigmenwechsel: Compliance als aktive Geschäftschance und nicht allein zur Risikoabwehr.*



Dr. Christian Schefold

### 1 Klassische IP-Rechte oder Geschäftsgeheimnisse?

Unternehmen, die mit ihren Erfindungen oder Produktgestaltungen die Veröffentlichung in Registern scheuten, haben schon immer versucht, mit einem konsequenten internen Regime Wissen im Unternehmen zu halten und seinen Abfluss nach außen zu unterbinden. Patente und Muster haben den Nachteil, dass sie veröffentlicht werden. Eine Ausnahme gilt nur für Staatsgeheimnisse – jedoch nur selten hat Know-how diese Qualität der Vertraulichkeit. Nach Veröffentlichung beträgt die Schutzdauer eines Patents in der Regel 20 Jahre nach Anmeldung. Bei Gebrauchsmustern ist die Dauer des Ausschließlichkeitsschutzes deutlich kürzer. Da das Wissen aufgrund der Registeröffentlichkeit offenkundig ist, kann es jeder schon vor Ablauf der Exklusivität zur Kenntnis nehmen und Parallelerfindungen starten. Nach Ablauf der Schutzfrist ist das Wissen dann frei verwendbar.

Wenn es nun gelingt, Know-how für ein Unternehmen zu erhalten und durch vertragliche, technische und organisatorische Maßnahmen dauerhaft zu schützen, so kann eine praktisch unbegrenzt lange, effektive Schutzdauer erreicht und auch gezielte Parallelerfindungen durch eine Geheimhaltung und entsprechende Verbote gegenüber Know-how-Trägern wirksam unterbunden werden. Als bestes Beispiel mag hier die Handhabung der berühmten Coca-Cola-Formel gelten: Wenn John Stith Pemberton seinen Kopfschmerzsirup 1886 zum Patent angemeldet hätte, wäre diese Weltmarke heute aller Voraussicht nach selbst in den USA wohl kaum bekannt geworden. Nicht jedes Know-how schafft die Bedeutung, die es dann zeitlos als Marke ausbeuten lässt. Grund genug, im Unternehmen aktiv für den Schutz von Geschäftsgeheimnissen zu sorgen!

\* Dr. Christian Schefold ist Rechtsanwalt und Partner bei Dentons Europe LL.P. in Berlin.

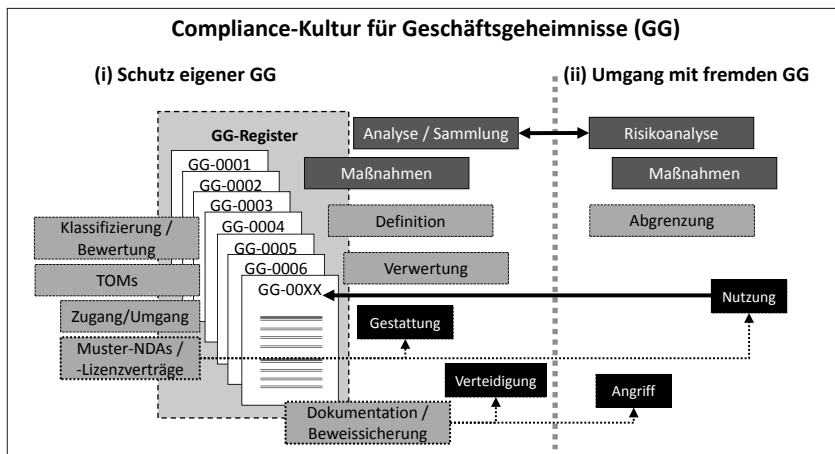


Abbildung 1: Compliance-Kultur für Geschäftsgeheimnisse

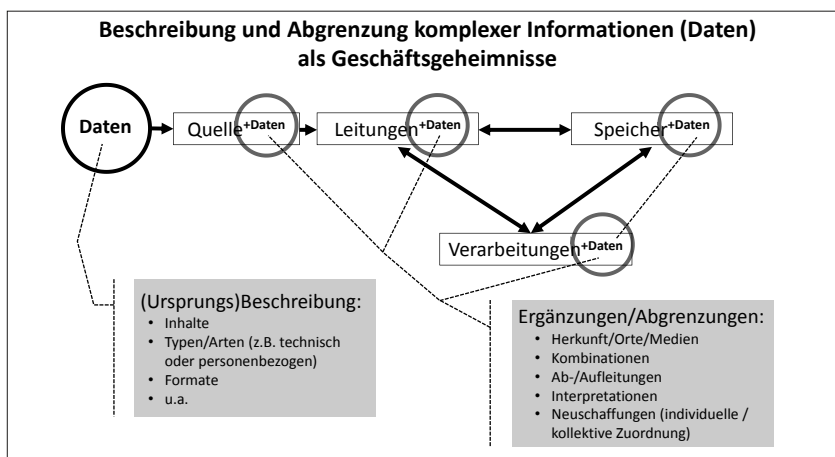


Abbildung 2: Beschreibung und Abgrenzung von Daten als Geschäftsgeheimnisse

## 2 Was nützt ein Geschäftsgeheimnis?

Geschäftsinformationen, die als Geschäftsgeheimnis anerkannt sind, dürfen grundsätzlich nicht von Unbefugten genutzt werden (§ 4 GeschGehG).<sup>1</sup> Ohne Mitwirkung des Inhabers dürfen diese weder erlangt, genutzt oder weiter offengelegt, das heißt veröffentlicht und verbreitet werden. Zuwiderhandlungen stehen unter Strafe (§ 23 GeschGehG). Unternehmen sind zudem für die Rechtsverletzungen durch Beschäftigte oder Beauftragte verantwortlich (§ 12 GeschGehG). Allein dieses Risiko zwingt Unternehmen bereits zu einer Geschäftsgeheimnis-Compliance; hier ganz traditionell als Risikoabwehr und nicht – wie noch auszuführen wird – um Geschäftschancen für das Unternehmen zu eröffnen.

Gegen Rechtsverletzer können ferner Auskunftsrechte, Beseitigungs- und Unterlassungsansprüche hinsichtlich des unbefugten Gebrauchs des Know-hows sowie die Vernichtung, die Herausgabe, ein Rückruf sowie Entfernung und Rücknahme vom Markt sowie natürlich auch Schadenersatz (nach dem Maßstab angemessener Lizenzgebühren) geltend gemacht werden (§§ 6 ff. GeschGehG). Die

Inanspruchnahme darf nicht unverhältnismäßig oder gar missbräuchlich sein; bei unverhältnismäßigen Nachteilen können sich Ansprüche auf Abfindungen in der Höhe angemessener Lizenzgebühren beschränken (§§ 11 und 14 GeschGehG). Für die Geltendmachung der Verteidigungsrechte gibt es nun das besondere Zivilverfahren für Geschäftsgeheimnistreitsachen (§§ 15 ff. GeschGehG).

Bisher beschränkte sich der Nutzen in der Regel auf den internen Bereich des Unternehmens: Da Know-how, wenn es einmal die Gewahrsamsphäre des Unternehmens verlassen hatte, nur schwer zu schützen war, bestand der klassische Schutz aus einem „Wegsperrn“ der „Verschlussache“, die damit nur einem ganz engen Kreis von Eingeweihten – oft nur dem Unternehmensinhaber – bekannt war. Werden nun bestimmte im GeschGehG festgelegte Voraussetzungen eingehalten, die am besten über ein gezielt auf den Umgang mit Geschäftsgeheimnissen ausgerichtetes Compliance-Management-System – ein GeschGeh-CMS – geschaffen werden, eröffnen sich dem Unternehmen Möglichkeiten, auf einer solchen Grundlage mit einem verbesserten Instrumentarium zur Handhabung von Geschäftsgeheimnissen und auch wirksamerer Rechtsverteidigung das eigene Know-how auch extern im weit stärkeren Maße zu schützen. Die Konsequenz wird sein, dass sowohl unternehmensintern Umgangsregeln aufgestellt aber auch mit Geschäftspartnern über den Umgang mit Geschäftsgeheimnissen verhandelt werden muss. Der Inhaber eines Geschäftsgeheimnisses kann den Zugang zu geschütztem Know-how, die Nutzung und auch weitere Verbreitung vertraglich präziser (wenn nicht vielleicht sogar erstmalig) gegenüber Dritten gestatten und hierfür Lizenzgebühren oder andere Gegenleistungen verlangen.

Damit wird wirtschaftlich die Verwertung von Geschäftsgeheimnissen verbessert und ein weiterer Anreiz für eine systematische Entwicklung, Verwaltung sowie auch Verwertung von Geschäftsgeheimnissen geschaffen. Geschäftsgeheimnisse können nun auch besser als Wert eines Unternehmens dargestellt und wirtschaftlich etwa als Sicherheit für die Kapitalaufnahme genutzt werden. Damit wird – vorausgesetzt es besteht ein GeschGeh-CMS – die wirtschaftliche Handlungsspielraum für Unternehmen erweitert.

Die Rechte aus Geschäftsgeheimnissen sind leider nicht unbeschränkt und ein neu gestaltetes Rechtsinstrument lädt auch zu neuen Überlegungen über Einschränkungen ein. Von Dritten eigen-

1 Das GeschGehG wird in diesem Beitrag nur zusammenfassend dargestellt. Für eine umfassendere Darstellung und tiefere Analyse wird auf Rehaag C./Straszewski, P., Das neue Gesetz zum Schutz von Geschäftsgeheimnissen in der Praxis, in: Mitteilungen der deutschen Patentanwälte, 2019, S. 249 ff. verwiesen.

**Compliance-Management erweitert nun die Nutzbarkeit von Geschäftsgeheimnissen.**

ständig entwickeltes Knowhow – vorausgesetzt es besteht eine entsprechende, über ein GeschGeh-CMS geschaffene Beweislage – wie auch ein rechtmäßiges Beobachten, Untersuchen, Rückbauen oder Testen schränkt die Durchsetzung von Rechten ein (§ 3 GeschGehG). Hier wird ein zukünftiger Regelungsbedarf bei Lizenzverträgen bestehen, um ein legales Aushebeln von Geschäftsgeheimnissen zu unterbinden. Es können ebenfalls nicht die Meinungs- und Informationsfreiheit, Arbeitnehmer- und Arbeitnehmervertretungsrechte sowie ein Aufdecken von Fehlverhalten (das Whistleblowing) allein durch ein Berufen auf Geschäftsgeheimnisse untersagt werden (§ 5 GeschGehG).

### 3 Wie entsteht ein Geschäftsgeheimnis?

Ein Geschäftsgeheimnis entsteht aus einer Wechselwirkung: Es ist über den jeweiligen Inhaber hinaus unbekanntes sowie auch unzugängliches Wissen – und daher wirtschaftlich wertvoll. Weil es einen Wert darstellt, wird es aber auch geheim gehalten. Dies setzt natürlich voraus, dass dieses Wissen beschreibbar ist, an sich einen Wert hat, geheim gehalten wird und ein berechtigtes Inte-

resse an seiner Geheimhaltung besteht (§ 2 Nr. 1 GeschGehG).

#### 3.1 Ein Geschäftsgeheimnis muss definiert werden

Hier helfen die Instrumente einer Risikoanalyse. Dabei gilt es im Unternehmen zu hinterfragen, was eigentlich das Betriebswissen ausmacht. Welches Know-how führt zu einem Wettbewerbsvorsprung? Auf welche Fertigkeiten ist die Produktion etwa stolz? Was sind die Ergebnisse von Forschung und Entwicklung – vor einer Patent- oder Musteranmeldung? Ähnlich einer Risikoanalyse helfen hier Workshops mit Know-how-Trägern, aber auch Interviews, Fragebögen und ein internes Meldewesen – zum Beispiel das in vielen Unternehmen vorhandene betriebliche Vorschlagswesen. Hier kann neben Entwicklung und Produktion auch der Vertrieb eine Rolle spielen. Im ständigen Kundenkontakt kennt der Vertrieb die Vorzüge von Produkten und Dienstleistungen. Dies sind Indikatoren für Know-how im Unternehmen. Oft liegen wertvolle Informationen in einem Unternehmen vor, ohne dass die wirtschaftliche Verwertbarkeit im Unternehmen bekannt ist und so Geschäftschan-

*Ein Compliance-Management verhilft zu einer Ausweitung des Geheimnisschutzes.*

cen bisher nicht wahrgenommen wurden. So stellt auch ein Wissen über Markt- und Wettbewerb ein Geschäftsgeheimnis dar, welches zudem einem Kartellverbot unterliegen kann. Damit hat eine solche Information eine ganz andere Wertigkeit, denn die Geheimhaltung hilft hier, schädigenden Einfluss einer Offenlegung zu verhindern. Nach einer solchen, umfassenden Analyse wird ein Unternehmen in der Lage sein, eine Liste von Geschäftsgeheimnissen zu erstellen. Diese Beschreibungen wertvoller Informationen sind die Grundlage eines Unternehmensregisters der Geschäftsgeheimnisse (siehe *Abbildung 1*).

### 3.2 Geschäftsgeheimnisse können vielseitig sein

Nicht nur das klassische Know-how spielt hier eine Rolle. Es können auch Informationen sein, die einen besonderen Wert darstellen, ohne selbst Wissen oder Know-how im engeren Sinne zu sein. Algorithmen – bisher in der Regel weder urheberrechtlich geschützt noch patentierbar – können sich nun als Geschäftsgeheimnis qualifizieren und so nicht nur geschützt, sondern auch besser verwertbar sein. Ein besonderes Feld der Information sind Daten. Dies gilt sowohl für personenbezogene als auch andere Daten. Die EU Datenschutzgrundverordnung (DSGVO) stellt nur besondere Beschränkungen für die Verarbeitung personenbezogener Daten auf, die zum Schutz der Persönlichkeitsrechte betroffener Individuen zu wahren sind. Die DSGVO sagt aber nichts über ein Eigentums- oder Besitzrecht an personenbezogenen Daten aus.

Ein zukünftiges Gestaltungs- und Anwendungsfeld können zum Beispiel Daten sein, die ein Unternehmen etwa durch seine Geschäftsaktivität, seine Anlagen und Geräte produziert. Die Herausforderung liegt hier schon in der Definition, der Beschreibung der Information als Schutzgegenstand eines Geschäftsgeheimnisses. Eine Definition stellt auch eine Abgrenzung dar – etwa gegenüber auf ähnliche Weise generierte Daten von Wettbewerbern, Zulieferern oder Kunden. Damit genügt nicht nur eine einfache Beschreibung für die Definition, es sind weitere Kriterien heranzuziehen, die für die gesamte Dauer und Wertschöpfungskette eines so begründeten Geschäftsgeheimnisses Gültigkeit behalten. Kann ein Geschäftsgeheimnis auf der Grundlage seiner Beschreibung nicht mehr identifiziert werden, etwa durch eine Vermischung mit anderen Daten, wird es allenfalls in der Kombination mit anderen Daten aber nicht mehr für sich allein einen Schutz in Anspruch nehmen und damit einen Wert darstellen können. Abgrenzungen individueller Geschäftsgeheimnisse aber auch das Entstehen gemeinsamer Geschäftsgeheimnisse sind dann in Lizenz- und Kooperationsverträge zu vereinbaren. Sofern es gelingt, Daten und insbe-

sondere auch personenbezogene Daten über alle Verarbeitungsprozesse abgrenzbar zu beschreiben, werden diese auch als Geschäftsgeheimnisse zu schützen sein (siehe *Abbildung 2*).

### 3.3 Geheim

Informationen werden nur dann geschützt, wenn sie in der Öffentlichkeit unbekannt sind und allgemein unzugänglich bleiben. Es sind damit Maßnahmen erforderlich, die dafür sorgen, dass Informationen geheim bleiben. Hier ist ein Rückgriff auf den Begriff der Technischen und Organisatorischen Maßnahmen aus dem Datenschutzrecht sinnvoll (Art. 32 DSGVO): Personenbezogene Daten dürfen ebenfalls nicht offenbart werden, der für ihre Verarbeitung Verantwortliche muss eine Offenlegung dieser besonderen Informationen vermeiden und für ein angemessenes Schutzniveau sorgen. Die Ausgangslage ist im neuen Recht der Geschäftsgeheimnisse die Gleiche wie im Datenschutzrecht: Die technische Sicherung erfordert eine Form des Abschließens – sowohl real als auch virtuell. Allerdings muss auch ein Zugang für bestimmte Personen bestehen und gewährleistet werden. Technische Zwischenfälle müssen bewältigt werden können (Stichworte: Cyber Security und IT-Sicherheit). Technische Vorkehrungen müssen konstant geprüft und gegebenenfalls auch verbessert werden. Organisatorische Sicherungen erfolgen durch Regelungen und Ordnungsverfahren für einen beschränkten beziehungsweise geregelten Zugang im Sinne eines Need-to-know für Mitarbeiter und Geschäftspartner. Hierfür sind vertragliche Maßnahmen (einschließlich arbeitsvertraglicher Maßnahmen) erforderlich, aber auch die Gestaltung von Arbeitsprozessen bis hin zur Kennzeichnung von Informationen als geheim – je nach Wert auch in unterschiedlichen Kategorien (beziehungsweise Stufen oder Klassen) von Geschäftsgeheimnissen. Auch hier kann eine Zuordnung über ein Unternehmensregister der Geschäftsgeheimnisse erfolgen.

## 4 Wie wird das eigene Geschäftsgeheimnis bewahrt?

Dies ist die Aufgabe eines GeschGeh-CMS: Die erste Maßnahme eines, auf Geschäftsgeheimnisschutz zugeschnittenen CMS ist unmittelbar mit der Analyse verbunden: Es folgt eine Definition beziehungsweise Beschreibung des Geschäftsgeheimnisses und seine Registrierung in einer Liste der Geschäftsgeheimnisse, dem schon genannten Unternehmensregister der Geschäftsgeheimnisse, dass damit auch ein Bestandsverzeichnis immaterieller Unternehmenswerte darstellt. Dieses Register kann der Vereinheitlichung wegen auch Patente und Muster sowie Marken als auch Belege für Urheberrechte enthalten. Ein derartiges Register dient

*Compliance-Tools  
helfen bei Erkennung,  
Definition und rechtssicherer  
Dokumentation  
von Geheimnissen.*

damit – ähnlich dem Verfahrensverzeichnis für personenbezogene Daten – als zentrale Datenbank für Unternehmenswerte einschließlich Informationen zum Umgang mit ihnen, das heißt den Schutzmaßnahmen, dem Kreis der Geheimnisträger und auch Regeln über die Einbindung weiterer Personen in den Kreis der Informierten und welche weitere Maßnahmen gegenüber Mitarbeitern aber auch Geschäftspartnern erforderlich sind. Dieses Register lässt sich auch in ein Verzeichnis der Lizenzen, der Verträge über eine Gestattung der Nutzung geistigen Eigentums gegenüber Dritten ausbauen. Bei vielen Unternehmen fehlt eine solche Übersicht über immaterielle Vermögenswerte, was bislang dazu führte, dass Unternehmenswerte in nicht unerheblichem Umfang nicht realisiert werden konnten oder gar verloren gingen. Das Register selbst wird auch ein Geschäftsgeheimnis sein.

Geschäftsgeheimnisse setzen zudem voraus, dass ein berechtigtes Interesse an ihrer Geheimhaltung besteht und sie einen wirtschaftlichen Wert haben. Daraus folgt zwingend eine Bewertung. Auf deren Grundlage lässt sich auch eine Klassifizierung eines Geschäftsgeheimnisses ermöglichen. Know-how mit geringerem Wert wird geringere Schutzmaßnahmen benötigen und kann einem größeren Kreis an Personen bekannt sein, als die Kronjuwelen des Unternehmenswissens. Bewertungen können sich allerdings auch mit der Zeit ändern. Deswegen ist hier eine periodische Anpassung in einem Prozess zu definieren. Für die Bewertung selbst wird sowohl Fachkenntnis über den Innovationsgehalt, den Exklusivitätswert, wie aber auch Markt- und Realisationswert gefordert.

Die konkrete Bewertung wird zunächst nach den wirtschaftlichen Interessen und Selbsteinschätzung des Unternehmens selbst erfolgen. Hierbei wird zum einen eine Rolle spielen, ob Informationen als Innovation oder Marktkenntnis Wettbewerbsvorteile sichern und verschaffen können.

Auch Informationen, deren unsachgemäße oder unbefugte Anwendung einen Schaden anrichten kann, haben einen Wert. Dies gilt insbesondere für kartellrechtlich relevante Informationen, deren Preisgabe ein Bußgeld oder Schadenersatzanforderungen nach sich ziehen und deren Anwendung damit einen Wert haben. Hiervon sind allerdings Informationen abzugrenzen, die entweder direkt schädigend eingesetzt werden oder aber Schäden verdecken und Inanspruchnahmen verhindern können. Hinsichtlich dieser Gruppe von Informationen muss angenommen werden, dass kein berechtigtes Interesse an einer Geheimhaltung besteht, sondern diese gerade offengelegt werden sollen. Diesem Umstand trägt unter anderem § 5 GeschGehG Rechnung.

Bewertungen von Know-how müssen aber auch in der weiteren Unternehmensrechnung berücksichtigt werden: Insbesondere bei der Bilanzierung kann sich durch wertvolle Geschäftsgeheimnisse die Passivseite verändern. Einerseits macht dies das Unternehmen wertvoller, erhöht Kapital und die Möglichkeit weiterer Kapitalaufnahmen – führt aber auf der anderen Seite zu einer Änderung der kapitalbezogenen Unternehmenskennziffern (zum Beispiel RoA/RoNA oder RoCE).<sup>2</sup>

Primär dient das Unternehmensregister der Geschäftsgeheimnisse der Dokumentation und Beweissicherung – auch zur eigenen Verteidigung. Hier sollten alle erforderlichen Informationen zusammenlaufen und verwaltet werden. In diesem Register werden auch die konkreten Maßstäbe

*Compliance betrifft die Schaffung eigener wie aber auch die Achtung fremder Geheimnisse.*

2 Return on Assets bzw. Return on Net Assets oder Return on Capital Employed – gebräuchliche Kennziffern um im Rahmen von Unternehmensanalysen die wirtschaftliche Potenz eines Unternehmens darzustellen. Hohe immaterielle Vermögenswerte, wie wertvolle Patente aber auch Geschäftsgeheimnisse können diese Kennziffern und damit die Bewertung des Unternehmens auch negativ beeinflussen.

für technische und organisatorische (Sicherungs-) Maßnahmen (TOMs) zugeordnet und definiert.

Insgesamt führen die bisher benannten Maßnahmen zu bestimmten Verhaltensvorgaben, die in einer Richtlinie zum Schutz eigener Geschäftsgeheimnisse zusammenzufassen sind. Diese Richtlinie legt idealer Weise kurz den Zweck dar, durch Geheimhaltung wertvoller Informationen das Unternehmensvermögen zu schützen aber auch auszubauen. Dann sollten in Kurzform Grundsätze des Verhaltens dargelegt werden, bestehende Maßnahmen und ihre Anwendung beschrieben sowie Dos und Don'ts definiert werden. Wenn eine Richtlinie zudem auch Hilfestellungen anbieten soll, können Hinweise für ein Verhalten in bestimmten Situationen gegeben werden. Diese Richtlinien sind dann nicht nur zur Dokumentation in Textform, sondern auch besser in Präsentationsform für ein Training oder Webinar verfügbar.

Unternehmensprozesse definieren das Onboarding neuer Mitarbeiter aber auch den Einsatz von Geheimnisschutzklauseln in Arbeitsverträgen, Abwägungskriterien und Handlungsempfehlungen für den Umgang mit Kündigungen von Geheimnisträgern, aber auch die Verwendung konkreter Vertraulichkeitsvereinbarungen (Non Disclosure Agreements – NDAs) sowie auch Nutzungsgestattungen (Lizenzverträge) gegenüber Lieferanten, Kunden und Kooperationspartnern. Das neue Gesetz hat auch Auswirkungen auf die bisher übliche Gestaltung von NDAs und Lizenzverträgen; insbesondere ist eine höhere Präzision gefragt. Hier muss in Zukunft ein größerer Wert auf die Darlegung des Hintergrundes beziehungsweise Zweck der Vereinbarung gelegt werden. Auch ist vor dem Hintergrund des Einsatzes das jeweils betroffene Geschäftsgeheimnis (mit Bezug um entsprechenden Unternehmensregister) darzulegen beziehungsweise zu definieren (Bezeichnung, Beschreibung, Abgrenzung – etwa im Hinblick auf bereits verfügbares Wissen). Geschäftspartner müssen selbst zu TOMs verpflichtet sein. Eine Nutzung des Geschäftsgeheimnisses ist nur für den dargelegten Zweck zu gestatten und jegliche andere Verwendung, wie auch eine Untersuchung oder ein Rückbau sollten untersagt werden. Darüber hinaus sollten die Regeln in Lizenzverträgen dann noch ausführlicher sein. Wie vorher bereits angesprochen, sind unter anderem für den Bestand eines Geschäftsgeheimnisses schädliche Maßnahmen, wie Beobachten, Untersuchen, Rückbauen oder Testen beziehungsweise etwaige Nutzungen daraus zu untersagen sowie die Kooperation bei neuen oder veränderten Geschäftsgeheimnissen zu regeln.

Zudem können auch Vermarktungsleitfäden eine Rolle spielen; schließlich wird das Geheimhalten an sich keinen Wettbewerbsvorteil bringen. Die bewusste Nichtnutzung eines Geschäftsgeheimnisses ist hingegen wirtschaftlich nicht verwertbar:

Geschäftsgeheimnisse sind aufgrund des Angemessenheitsgebots und Missbrauchsverbot anders als Patente nicht zu einer Blockade geeignet.

## 5 Wie werden Verletzungen fremder Geschäftsgeheimnisse verhindert?

Der Schutz eigener Geschäftsgeheimnisse ist nur eine Seite der Medaille – ein Unternehmen möchte auch nicht wegen Verletzung fremder Geschäftsgeheimnisse in Anspruch genommen werden. Mit dem neuen GeschGehG sind Unternehmen auch für Rechtsverletzungen ihrer Mitarbeiter und Beauftragten verantwortlich. Daher ist hier, aus Risikogesichtspunkten ein gesondertes Augenmerk anzulegen. Ein Unternehmen, das selbst großen Wert auf den Schutz eigenen Know-hows Wert legt wird auch das Know-how anderer beachten. Damit stehen beide Ansätze, der Schutz eigener Geschäftsgeheimnisse und die Achtung fremder, in einem Gegenständigkeitsverhältnis – und stellen auch die Essenz einer Compliance-Kultur für Unternehmen dar.

Hier kann ein klassischer Compliance-Ansatz verfolgt werden: Risikoanalyse und thematische Ausrichtung eines Systems, Maßnahmen zur Risikoreduzierung wie Verhaltensrichtlinien und Unternehmensprozesse, Kommunikation einschließlich Schulungen – sowie last, but not least eine kontinuierliche Prüfung und Optimierung. Notwendigerweise wird der Aufbau – von einigen Ausnahmen abgesehen – nicht synchron mit einem System zum Schutz eigener Rechte laufen. Sinnvoll ist es etwa, in das Unternehmensregister auch fremde Geschäftsgeheimnisse aufzunehmen, deren Nutzung das Unternehmen legal erworben hat.

Ein wirksamer Schutz vor Inanspruchnahme Dritter wird letztendlich aber nur durch eine gelebte Compliance-Kultur der gegenseitigen Achtung von Geschäftsgeheimnissen und anderen gewerblichen Schutzrechten gesichert. Diese grundsätzliche Haltung sollte durch die Schärfung des Erkennens kritischer Situationen verstärkt werden. Dabei ist kein vorbehaltloses Anerkennen zweifelhafter Rechte Dritter gefordert – das GeschGehG gibt Unternehmen auch die Möglichkeit, kritischen Geschäftsgeheimnissen wirksam entgegenzutreten. So wäre beim Kontakt mit Know-how von Dritten zunächst der Bestand dieses Know-hows zu prüfen. Wie erfolgte die Offenlegung? Hat der Dritte überhaupt ausreichende Maßnahmen getroffen, um die Information als Geschäftsgeheimnis schützen zu können? Gibt es eigenständige Entdeckungen oder Schöpfungen, die dem Know-how des Dritten entsprechen? War das eigene Verhalten vielleicht ein zulässiges Beobachten, Untersuchen, Rückbauen oder Testen? Gibt es vertragliche Vereinbarungen oder Einschränkungen? Hier hilft erneut auch der Rückgriff auf ein Unternehmensregister der Geschäftsgeheimnisse. Damit lässt sich auch eine

*Eine Compliance-Organisation kann jetzt aktiv Werte im Unternehmen schaffen – ein Paradigmenwechsel.*

Entscheidung über eine Nutzung (mit oder ohne vertraglicher Regelung) oder gar den Angriff gegen ein fremdes Recht treffen.

Sinnvoll ist es, wenn eine Richtlinie zum Umgang mit fremden Geschäftsgeheimnissen den Zweck der Schadensvermeidung und den Grundsatz des rechtskonformen Verhaltens im Unternehmen definiert, wobei hier eine Checkliste zur Prüfung rechtmäßigen Alternativverhaltens dargestellt werden kann. Letztendlich ist auch hier eine Dokumentation entscheidend, um sich als Unternehmen gegen – hoffentlich – unberechtigte Vorwürfe zu verteidigen aber auch gegen unberechtigtes Geschäftsverhalten vorzugehen.

Schulungen sind hier ebenfalls geboten – insbesondere bei der Neueinstellung von Know-how-Trägern von Wettbewerbern, einschließlich Zulieferern und Kunden. Mag es früher üblich gewesen sein, dass ein Wechsel mit vollen Zeichnungsmappen und Datenboxen erfolgte, so wird dies heute nicht mehr möglich sein. Dies gilt in gleichen Maßen auch für den Wechsel von Zulieferern und Beratern; hier muss sichergestellt sein, dass kein geschütztes Wissen in illegaler Weise vermittelt wird. Um Risiken zu vermeiden ist durch einen entsprechenden Compliance-Ansatz erhöhte Wachsamkeit erforderlich.

## 6 Wer setzt das alles im Unternehmen um?

Die Compliance-Organisation ist grundsätzlich dazu geschaffen, Rechtsrisiken im Unternehmen aufzuspüren, entsprechende Maßnahmen einzuführen, Unternehmensbereiche bei den Maßnahmen zu unterstützen, diese zu überwachen und auf diese Weise Compliance stetig im Unternehmen zu verbessern. Die Themen einer Richtlinie zum Umgang mit fremden Geschäftsgeheimnissen sind in diesem Sinne Risikoprävention und gehören damit zu Compliance. Compliance wird sich dabei der fachlichen Unterstützung der Rechtsabteilung sowie hier insbesondere auch der Patentabteilung oder weiterer IP-Rechtler bedienen müssen.

Der Umgang mit eigenen Geschäftsgeheimnissen im Unternehmen ist – sofern es nicht allein die TOMs betrifft – hingegen keine klassische Risikovorsorge mehr. Der Schwerpunkt liegt hier auf einer Wahrung von Chancen und setzt damit auch einen anderen Ansatz voraus. Compliance als Funktion hat nun im Hinblick auf die Umsetzung des GeschGehG die Chance, sich in einen Unternehmensbereich zu entwickeln, der aktiv Werte für ein Unternehmen schafft. Dies ist in mehrfacher Hinsicht ein Paradigmenwechsel. Gerade wenn zum Bereich Compliance auch der Datenschutz gehört, wird Compliance ausreichend Erfahrung mit bestehenden Instrumenten (zum Beispiel Verfahrensverzeichnis, Richtlinien, Compliance-Prozesse) haben,

um das Thema Geschäftsgeheimnisse ebenfalls zu übernehmen. Für die fachliche Seite sind allerdings umfangreiche Kenntnisse im gewerblichen Rechtsschutz unabdingbar. In der Regel fehlen aber den entsprechenden Rechts- und Patentfunktionen die operative Erfahrung im Umsetzen rechtlicher Anforderungen. Hier liegt die Stärke von Compliance – und nun auch die Chance, aktiv Mehrwert im Unternehmen zu schaffen.

Die größte Herausforderung wird jedoch ein offensiver Umgang mit der Materie sein – nicht eher passiv Risiken zu vermeiden, sondern aktiv Chancen für das Unternehmen zu gestalten. Hier ist möglicherweise ein neuer Typ von Compliance Officer gefragt.

## 7 Next Steps

Compliance in Zusammenarbeit mit Entwicklungs- und Rechts-/Patentabteilungen hat nun folgende Aufgaben vor sich:

1. Förderung einer Unternehmenskultur der Achtung gewerblicher Schutzrechte und insbesondere Geschäftsgeheimnisse.
2. Sammlung von Geschäftsgeheimnissen (Analyse):
  - ▶ Technik, Wissen (insbesondere Vorstatus von Patenten), Daten,
  - ▶ Methoden und Verfahren (zum Beispiel Sammlung, Aufbereitung und Zurverfügungstellung von Informationen),
  - ▶ Geschäfts- und Marketingstrategien (zum Beispiel Vermarktungsmethoden, kartellrechtlich relevante Informationen).
3. Aufbau eines Unternehmensregisters für Geschäftsgeheimnisse (Maßnahme):
  - ▶ Verzeichnis der Schutzrechte (Beschreibung/Abgrenzung),
  - ▶ Bewertung/Klassifizierung/Zuordnung von Umgangsregeln,
  - ▶ Verhaltensempfehlungen/Vertragsmuster,
  - ▶ Dokumentation von Geschäftsvorgängen.
4. Entwurf/Verabschiedung von Richtlinien zum Umgangsregelungen mit
  - a. eigenen Geschäftsgeheimnissen:
    - ▶ Identifikation, Dokumentation und Kennzeichnung,
    - ▶ Unternehmensregister,
    - ▶ Vermarktung (Chancen),
    - ▶ Zuständigkeiten im Unternehmen.
  - b. Umgangsregelung zu fremden Geschäftsgeheimnissen:
    - ▶ Erkennen fremder Geschäftsgeheimnisse,
    - ▶ Bewertung fremder Geschäftsgeheimnisse,
    - ▶ Umgangsregeln (Risikoprävention),
    - ▶ Zuständigkeiten im Unternehmen.
5. Überwachung und Optimierung.

*Was sollte Compliance nun tun, um Chancen für das Unternehmen zu wahren?*