www.betriebs-berater.de

BB

Betriebs Berater

46 | 2019

Steuern ... GeschGehG ... Unternehmenssteuerreform ... IFRS ... Vertrauensarbeitszeit ...

11.11.2019 | 74. Jg.
Seiten 2689–2752

BB-Rechtsprechungsreport Gemeinnützigkeits- und Spendenrecht 2019

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Im Ergebnis ist festzuhalten, dass Kommunikation und Recht Schlüsselressourcen und Erfolgsfaktoren im Krisenfall sind. Werden sie synchronisiert eingesetzt, unterstützen sie eine erfolgreiche Krisenbewältigung und stärken damit die Reputation des Unternehmens.

Suntka von Halen ist Director bei der strategischen Kommunikationsberatung Brunswick Group. Sie berät globale Unternehmen u. a. in den Bereichen Krisenvorbereitung und Krisenkommunikation, Restrukturierung und Change.

Anne Baranowski, LL.M., RAin und FAin im IT-, Urheber- und Medienrecht bei Schalast Rechtsanwälte Notare in Frankfurt a. M. Sie betreut Mandanten insbesondere im IT-, Datenschutz- und Urheberrecht mit einem Schwerpunkt auf der Technologie- und Medienbranche.

Dr. Udo Kornmeier, RA, ist Partner bei Schalast Rechtsanwälte Notare und betreut Mandanten insbesondere im Urheber- und Medienrecht sowie im Bereich International Litigation.

Ingrid Burghardt-Richter, RAin/FAinHaGesR, und Dr. Johannes Bode, RA

Geschäftsgeheimnisschutzgesetz: Überblick und Leitfaden für Unternehmen zur Wahrung ihrer Geschäftsgeheimnisse

Am 26.4.2019 trat das Gesetz zum Schutz von Geschäftsgeheimnissen (Geschäftsgeheimnisschutzgesetz, „GeschGehG") in Kraft. Das Gesetz dient der Umsetzung der „Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung" („Know-how Richtlinie") (EU) 2016/943. Mit Hilfe des neuen Gesetzes können Unternehmen den Schutz ihrer Geschäftsgeheimnisse effektiver durchsetzen. Um allerdings in den von diesem Gesetz gewährten Schutz vor rechtswidriger Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen zu gelangen, enthält das Gesetz einige Neuerungen, die Unternehmen dringend berücksichtigen sollten.

I. Einleitung

Zu den wichtigsten Neuerungen durch das Geschäftsgeheimnisschutzgesetz zählt die in § 2 Nr. 1 GeschGehG enthaltene Legaldefinition des „Geschäftsgeheimnisses", worunter auch das in der Praxis bedeutende technische Wissen (Know-how) fällt. Der Rückgriff auf das bisherige naturgemäß lückenhafte Richterrecht wird hierdurch abgelöst. Das hat seinen Preis: Denn die zentrale Neuerung in der Definition des Geschäftsgeheimnisses liegt darin, dass nunmehr die zu schützende Information Gegenstand von „*angemessenen Geheimhaltungsmaßnahmen*" sein muss. Der Inhaber des Geschäftsgeheimnisses ist hierfür im Streitfall beweisbelastet. Dadurch werden die Anforderungen an den Geheimnisschutz im Vergleich zur früheren Rechtslage deutlich verschärft.

Positiv hervorzuheben ist die Vereinheitlichung der Regelungen zur Durchsetzung von Ansprüchen bei Rechtsverletzungen (rechtswidrige Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen).[1] Diese sind im zweiten Abschnitt in den §§ 6 bis 14 GeschGehG ähnlich der Verletzung gewerblicher Schutzrechte wie Unionsmarken und europäischer Patente geregelt. Danach können dem betroffenen Unternehmen weitreichende Ansprüche zustehen, wie Beseitigungs- und Unterlassungsansprüche oder Auskunfts- und Schadensersatzansprüche. Beachtenswert ist ferner, dass die betroffenen Unternehmen nunmehr auch Ansprüche auf Vernichtung, Herausgabe, Rückruf, Entfernung und Rücknahme der rechtsverletzenden Produkte vom Markt haben.

Schließlich birgt das Geschäftsgeheimnisschutzgesetz in Umsetzung des Art. 9 der Know-how-Richtlinie auch einige verfahrensrechtliche Neuerungen. Bestand zuvor das Risiko, Geschäftsgeheimnisse während eines Prozesses preisgeben zu müssen, wird dem nunmehr durch das neue Verfahren in Geschäftsgeheimnisstreitsachen des dritten Abschnitts in den §§ 15 bis 22 GeschGehG Rechnung getragen. Dabei kann das Gericht nach § 16 GeschGehG geheimhaltungsbedürftige Informationen auch als solche einstufen. In diesem Fall sind derartige Informationen während und auch nach dem Gerichtsverfahren von allen Beteiligten vertraulich zu behandeln.

II. Wesentliche Neuerungen durch das Geschäftsgeheimnisschutzgesetz

Der zuvor bloß mosaikartige Schutz der Geschäftsgeheimnisse wird durch das Geschäftsgeheimnisschutzgesetz grundlegend reformiert und umfassend in einem eigenen Spezialgesetz geregelt.

1 Vgl. *Lamy/Vollprecht*, IR 2019, 201, 204.

1. Definition des Geschäftsgeheimnisses

Nach der in § 2 Nr. 1 GeschGehG enthaltenen Definition ist ein Geschäftsgeheimnis

„eine Information

a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht."

a) Information

Unter Information sind nicht nur das technische Know-how (bisher Betriebsgeheimnisse) zu fassen, sondern auch die kaufmännischen Informationen des Unternehmens (bisher Geschäftsgeheimnisse).[2] Von dem weit auszulegenden Begriff der Information wird daher sowohl technisches als auch kaufmännisches Wissen umfasst. Diese Begriffsbestimmung soll im Einklang mit der bisherigen Rechtsprechung stehen und solche Informationen schützen, an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat.[3]

b) Fehlende Offenkundigkeit und wirtschaftlicher Wert

Die Information darf nach § 2 Nr. 1a) GeschGehG nicht offenkundig sein, gemessen am allgemeinen Bekanntheitsgrad.[4] Dabei kommt es auf die Unbekanntheit in Kreisen an, die üblicherweise mit dieser Art von Informationen umgehen. Dies ist im Ergebnis jedoch nichts Neues. Sobald eine Information in den betreffenden Fachkreisen bekannt wurde, gingen die Gerichte auch nach früherer Rechtslage von Offenkundigkeit aus.[5]

Nicht notwendig war bisher allerdings, dass der Information ein eigener wirtschaftlicher Wert zugemessen wurde.[6] Es genügte nach alter Rechtslage vielmehr, dass die Information eine Verbindung zur Geschäftstätigkeit des Geheimnisträgers aufwies und an deren Geheimhaltung ein berechtigtes (wirtschaftliches) Interesse bestand.[7] Eine bestimmte Wertschwelle war nicht vorausgesetzt, wenn die Information nur auf irgendeine Weise kommerziell verwertbar war.[8] Nach der neuen Definition werden dagegen nur solche Informationen geschützt, die von kommerziellem Wert sind, gerade weil sie geheim sind. Das ist der Fall, *„wenn die Erlangung, Nutzung oder Offenlegung [der Information] ohne Zustimmung des Inhabers dessen wissenschaftliches oder technisches Potenzial, geschäftliche oder finanzielle Interessen, strategische Position oder Wettbewerbsfähigkeit negativ beeinflussen"*.[9] Damit scheiden belanglose ebenso wie rein private Informationen, die nicht im geschäftlichen Verkehr verwertbar sind, aus dem Anwendungsbereich des Geschäftsgeheimnisschutzgesetzes aus.[10]

c) Gegenstand von angemessenen Geheimhaltungsmaßnahmen

Von zentraler Bedeutung innerhalb der Definition des Geheimnisbegriffs ist, dass die geheim zu haltende Information Gegenstand von *„angemessenen Geheimhaltungsmaßnahmen"* sein muss. Daraus leitet sich der Maßstab dafür ab, wie Unternehmen in Zukunft agieren müssen, damit die unternehmensinternen Informationen im Sinne des Geschäftsgeheimnisschutzgesetzes geschützt sind. Bisher wurde das Bestehen eines Geheimhaltungs*willens*, dessen Vorliegen sogar vermutet wurde, als ausreichend erachtet.[11] Nach neuer Rechtslage muss sich dieser Wille nunmehr in der *Durchführung konkreter und „angemessener Geheimhaltungsmaßnahmen"* niederschlagen.[12] Das hat letztlich zwei wesentliche Konsequenzen: Erstens müssen Unternehmen aktiv tätig werden, um auch weiterhin in den Genuss des Geheimnisschutzes zu kommen,[13] was zweitens dazu führt, dass sich die Geschäftsleitung bei Unterlassen „angemessener Geheimhaltungsmaßnahmen" einem *persönlichen Haftungsrisiko* ausgesetzt sehen könnte.[14]

Was genau unter „angemessenen Geheimhaltungsmaßnahmen" zu verstehen ist, wird im Geschäftsgeheimnisschutzgesetz nicht definiert und ist eine Frage des jeweiligen Einzelfalls.[15] Jedenfalls muss es sich um Maßnahmen handeln, die im Einzelfall angemessen sind. Sie müssen aber nicht absolut wirksam, unumgehbar oder gar optimal sein.[16] Das bedeutet, dass jeweils im Einzelfall ein variabler Maßstab anzulegen ist, wenn es um die Beurteilung der Angemessenheit der Maßnahmen geht. Dafür sind verschiedene Kriterien beachtlich,[17] wie beispielhaft

- die Schutzwürdigkeit der Information, ihr Wert bzw. die Bedeutung für das Unternehmen und die Art bzw. Natur der Information sowie Entwicklungskosten einer Information,
- die Größe des Unternehmens und dessen wirtschaftliche Kapazitäten und verfügbare Mittel,
- Kosten und Üblichkeit der Maßnahme (im Unternehmen), die Art der Kennzeichnung der Informationen und vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern sowie
- die Größe eines potentiellen Schadens durch Verlust der Information.

Einen ansatzweise verlässlichen Maßstab für die Angemessenheit der Maßnahme wird es allerdings erst mit zukünftiger höchstrichterlicher Rechtsprechung geben.

d) Berechtigtes Interesse

Mit dem berechtigten Interesse hat der Gesetzgeber eine weitere Voraussetzung des Geschäftsgeheimnisbegriffs in das Gesetz eingefügt, die weder in der Know-how-Richtlinie noch im Regierungsentwurf enthalten war. Hintergrund dessen war die Sorge, dass ansonsten auch „illegale Machenschaften" in den Schutzbereich fallen könnten.[18] In der Literatur sind die Konsequenzen dieses Vorstoßes um-

2 So ausweislich der Regierungsbegründung BT-Drs. 19/4724, 24; *Lamy/Vollprecht*, IR 2019, 201, 202; *Ohly*, GRUR 2019, 441, 442.
3 BT-Drs. 19/4724, 24; ebenso *Ohly*, GRUR 2019, 441, 442.
4 *Rosenthal/Hamann*, NJ 2019, 321, 322; *Hauck*, GRUR-Prax 2019, 223, 224; *Ohly*, GRUR 2019, 441, 442.
5 *Gregor*, ZCG 2016, 262 f.; *Heinzke*, ZCG 2016, 262 f.
6 *Rosenthal/Hamann*, NJ 2019, 321, 322; *Ohly*, GRUR 2019, 441, 443.
7 *Heinzke*, ZCG 2016, 262, 182.
8 *Heinzke*, ZCG 2016, 262, 182.
9 BT-Drs. 19/4724, 24.
10 BT-Drs. 19/4724, 24; *Lamy/Vollprecht*, IR 2019, 201, 202; *Ohly*, GRUR 2019, 441, 442 f.
11 *Otte-Gräbener/Kutscher-Pius*, ZVertriebsR 2019, 288, 289; *Dann/Markgraf*, NJW 2019, 1774, 1775; *Ohly*, GRUR 2019, 441, 443.
12 *Lamy/Vollprecht*, IR 2019, 201, 203.
13 *Maaßen*, GRUR 2019, 352, 355 f.; *Rath/Schreiner/Laoutoumai*, Erste Hilfe zum Geschäftsgeheimnisschutzgesetz (GeschGehG), 2019, S. 7; *Freckmann/Schmoll*, BB 2017, 1780, 1781; *Ohly*, GRUR 2019, 441, 443.
14 *Dann/Markgraf*, NJW 2019, 1774, 1775.
15 *Dann/Markgraf*, NJW 2019, 1774, 1775; *Freckmann/Schmoll*, BB 2017, 1780, 1781; *Lamy/Vollprecht*, IR 2019, 201, 203.
16 *Maaßen*, GRUR 2019, 352, 353 f.; *Ohly*, GRUR 2019, 441, 443; *Otte-Gräbener/Kutscher-Pius*, ZVertriebsR 2019, 288, 289; *Dann/Markgraf*, NJW 2019, 1774, 1775 f.
17 Vgl. die verschiedenen Kriterien bei: BT-Drs. 19/4724, 24; *Maaßen*, GRUR 2019, 352, 354; *Ohly*, GRUR 2019, 441, 444; *Lamy/Vollprecht*, IR 2019, 201, 203; *Rosenthal/Hamann*, NJ 2019, 321, 323.
18 *Ohly*, GRUR 2019, 441, 444; *Lamy/Vollprecht*, IR 2019, 201, 204.

stritten, insbesondere wird vertreten, dass diese Regelung mit der Know-how Richtlinie unvereinbar ist.[19] Unabhängig davon bliebe ein möglicher Anwendungsbereich ohnehin gering.

2. Anspruchsbegründende rechtswidrige Verletzungshandlungen

Um Ansprüche aus dem Geschäftsgeheimnisschutzgesetz geltend zu machen, muss ein Geschäftsgeheimnis rechtswidrig erlangt, genutzt oder offengelegt werden. Hierzu enthalten die §§ 3 bis 5 GeschGehG ausdrückliche Regelungen.

a) Handlungsverbote nach § 4 GeschGehG

Zunächst darf – vereinfacht ausgedrückt – ein Geschäftsgeheimnis nach dem sehr weit gefassten Tatbestand des § 4 Abs. 1, Abs. 2 Nr. 1 GeschGehG nicht auf unzulässigem Wege erlangt und anschließend genutzt oder offengelegt werden.[20] Wichtiger ist allerdings, dass ein Geschäftsgeheimnis, das rechtmäßig erlangt wurde (z. B. bei freiwilliger Weitergabe an Vertragspartner), nicht genutzt oder offengelegt werden darf, wenn dies gegen vertragliche Verpflichtungen (z. B. Vertraulichkeitsvereinbarungen) verstößt, vgl. § 4 Abs. 2 Nr. 2 und 3 GeschGehG.

Im Hinblick auf Vertraulichkeitsvereinbarungen ist insbesondere zu beachten, dass eine Nutzung oder Offenlegung der Information nur rechtswidrig ist und zu Ansprüchen nach den §§ 6 bis 14 GeschGehG führen kann, wenn auch tatsächlich ein Geschäftsgeheimnis vorliegt. Die Vertraulichkeitsvereinbarung allein genügt nicht, um eine Information zu einem Geschäftsgeheimnis werden zu lassen. Sie kann allenfalls eine von verschiedenen „angemessenen Geheimhaltungsmaßnahmen" darstellen. Treffen Unternehmen daneben keine weiteren Maßnahmen, ist die Vertraulichkeitsvereinbarung (wenn sie wie heutzutage üblich ohne Vertragsstrafe vereinbart wurde) nicht mehr als ein zahnloser Tiger.

b) Erlaubte Handlungen nach § 3 GeschGehG

Erlaubt ist dagegen die Erlangung, Nutzung oder Offenlegung eines Geschäftsgeheimnisses in den vom Gesetzgeber geschaffenen, nicht abschließenden Fallgruppen des § 3 GeschGehG.[21] Dabei bilden diese Fallgruppen im Wesentlichen die bisher gängige Praxis ab. So ist insbesondere die Parallelschöpfung (§ 3 Abs. 1 Nr. 1 GeschGehG) und der gesetzlich vorgeschriebene bzw. vertragliche Erwerb (§ 3 Abs. 1 Nr. 3 und Abs. 2 GeschGehG) von Geschäftsgeheimnissen zulässig. Als weitere Möglichkeit, rechtmäßig Geschäftsgeheimnisse zu erwerben, wird das in Deutschland bisher unzulässige „*Reverse Engineering*" nunmehr grundsätzlich erlaubt (§ 3 Abs. 1 Nr. 2 GeschGehG). Dies führt zu einem geringeren Schutz für Geschäftsgeheimnisse.[22] Im Geschäftsgeheimnisschutzgesetz heißt es dazu:

„Ein Geschäftsgeheimnis darf insbesondere erlangt werden durch ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der

a) öffentlich verfügbar gemacht wurde oder

b) sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt."

Aus dem letzten Satz ist zu schließen, dass das Reverse Engineering vertraglich verboten werden kann, etwa als Inhalt einer Geheimhaltungsvereinbarung (siehe III. 2. c)).

c) Ausnahmen nach § 5 GeschGehG (insb. Whistleblowing)

Darüber hinaus ist nach § 5 GeschGehG die Erlangung, Nutzung oder Offenlegung einer Information trotz eines Verstoßes gegen § 4 GeschGehG zulässig, wenn dies dem Schutz eines berechtigten Interesses dient. Die generalklauselartig formulierte Ausnahme soll gerade den investigativen Journalismus schützen. Nach § 5 Nr. 2 GeschGehG wird insbesondere das sog. „*Whistleblowing*" zugelassen, also die Erlangung, Nutzung oder Offenlegung

„zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen".

Der Gesetzgeber weicht damit von der Know-how-Richtlinie ab, die noch verlangte, dass der Erwerb, die Nutzung oder die Offenlegung für die Aufdeckung erforderlich ist und in der Absicht gehandelt wird, öffentliche Interessen zu schützen.[23] Dementgegen soll eine solche Gesinnungsprüfung nach deutschem Recht vermieden werden und ausreichen, dass der Whistleblower zumindest einen hinreichenden Anlass zur Aufdeckung des Fehlverhaltens hatte.[24]

3. Rechtsfolgen (Ansprüche) und Verfahren

Aufgrund einer Rechtsverletzung können den betroffenen Unternehmen als Geheimnisinhabern (§ 2 Nr. 2 GeschGehG) umfassende und ausdifferenzierte Ansprüche des zweiten Abschnitts §§ 6 bis 14 GeschGehG gegen den Rechtsverletzer (§ 2 Nr. 3 GeschGehG) zustehen und nach dem neuen Verfahren als Geschäftsgeheimnisstreitsache geltend gemacht werden.

a) Ansprüche bei Rechtsverletzungen

Ansprüche bei Rechtsverletzungen sind im Einzelnen

- ein Anspruch auf Beseitigung und Unterlassung nach § 6 GeschGehG,
- ein Anspruch auf Vernichtung, Herausgabe, Rückruf, Entfernung und Rücknahme vom Markt nach § 7 GeschGehG
- das Auskunftsrecht über rechtsverletzende Produkte sowie auf Schadensersatz bei fehlerhafter oder nicht erfolgter Auskunft nach § 8 GeschGehG,
- ein allgemeiner Schadensersatzanspruch bei Verletzungen eines Geschäftsgeheimnisses nach § 10 GeschGehG und
- ein spezieller bereicherungsrechtlicher Herausgabeanspruch nach § 13 GeschGehG, der den § 7 GeschGehG insoweit ergänzt, dass eine Herausgabe auch nach Verjährung des Schadensersatzanspruchs noch möglich ist.

Gegen die Geltendmachung der in §§ 6 bis 8 Abs. 1 GeschGehG normierten Ansprüche kann nach § 9 GeschGehG eingewendet werden, dass die Geltendmachung unverhältnismäßig ist (z. B. kann es unverhältnismäßig sein, vom Rechtsverletzer eine Entfernung und Rücknahme vom Markt zu verlangen, wenn das betroffene Unternehmen das Geschäftsgeheimnis selber nicht nutzt).[25] Dem ausdrücklichen Wortlaut des § 9 GeschGehG zufolge gilt der Unverhältnismäßigkeits-

19 Vgl. *Gärtner/Oppermann*, BB 35/2019, „Die Erste Seite"; *Ohly*, GRUR 2019, 441, 444.
20 Vgl. *Lamy/Vollprecht*, IR 2019, 201, 204.
21 BT-Drs. 19/4724, 25.
22 *Heinzke*, ZCG 2016, 262, 180.
23 *Gaugenrieder*, BB 2014, 1987, 1991.
24 *Ohly*, GRUR 2019, 441, 448.
25 *Ohly*, GRUR 2019, 441, 449.

einwand nur für die Ansprüche der §§ 6 bis 8 Abs. 1 GeschGehG, nicht aber für den Schadensersatzanspruch nach § 10 GeschGehG.

b) Verfahren als Geschäftsgeheimnisstreitsache

Die dargestellten Ansprüche können nunmehr im Verfahren als Geschäftsgeheimnisstreitsache geltend gemacht werden; sie sind dann auch während eines Gerichtsverfahrens grundsätzlich vertraulich zu behandeln. Nach § 16 Abs. 1 GeschGehG kann das Gericht Informationen als geheimhaltungsbedürftig einstufen. Damit sind sämtliche Beteiligte verpflichtet, diese Informationen, teilweise sogar über den Abschluss des Verfahrens hinaus, vertraulich zu behandeln (§§ 16 Abs. 2, 18 GeschGehG). Ferner kann das Gericht nach § 19 GeschGehG entsprechende Maßnahmen zum Schutz der Vertraulichkeit treffen, wie Zugangsbeschränkungen zu Dokumenten, den Ausschluss von Prozessbeteiligten und sogar den Ausschluss der Öffentlichkeit.

III. Handlungsvorschläge

Um die zu schützenden unternehmenseignen Informationen als Geschäftsgeheimnisse sicherzustellen, müssen „angemessene Geheimhaltungsmaßnahmen" ergriffen werden. Dementsprechend sind betroffene Unternehmen gut beraten, wenn sie jedenfalls die folgenden drei Schritte durchführen:

1. Bestandsaufnahme/Ermittlung des status quo
   a) Ermittlung aller zu schützenden Informationen und den hierfür verantwortlichen Personen
   b) Bewertung des aktuellen Schutzstandards
2. Implementierung eines Geheimnisschutzkonzepts
   a) Kategorisierung der Informationen nach ihrer Schutzwürdigkeit
   b) Festlegung „angemessener Geheimhaltungsmaßnahmen"
3. Umfangreiche Dokumentation sowie regelmäßige Evaluation und Anpassung der „angemessenen Geheimhaltungsmaßnahmen"

Nur so können die (Abwehr-)Ansprüche entstehen, bei Bedarf geltend gemacht und das Vorliegen „angemessener Geheimhaltungsmaßnahmen" bewiesen werden.

1. Bestandsaufnahme/Ermittlung des status quo

Im ersten Schritt sollten sämtliche unternehmensinternen Informationen, die eines besonderen Schutzes bedürfen, lokalisiert und gewissenhaft aufgelistet werden. Dabei ist im Hinblick auf die Beurteilung der notwendigen „angemessenen Geheimhaltungsmaßnahmen" darauf zu achten, welche Personen Zugang zu den Informationen haben. Als vorbereitende Maßnahme für die folgenden Schritte kann hierbei zugleich das Augenmerk auf eventuell bereits bestehende Schutzlücken gelegt werden.[26]

2. Implementierung eines Geheimnisschutzkonzepts

In einem zweiten Schritt sollte sodann ein Geheimnisschutzkonzept im Einklang mit den bereits bestehenden Konzepten im Datenschutz (vgl. Art. 32 DSGVO) oder im Bereich der IT-Sicherheit (vgl. u. a. § 8a BSIG) geschaffen werden. Mögliche Synergien können und sollten genutzt werden. Dabei hängen Umfang und Notwendigkeit eines Geheimnisschutzkonzepts stark von den Umständen des Einzelfalls ab (z. B. der Größe des Unternehmens, die Menge vertraulicher Informationen und/oder der Anzahl der Mitarbeiter). Ein mögliches Konzept könnte die Einteilung vertraulicher Informationen in verschiedene Kategorien und die Festlegung des Schutzniveaus für die jeweiligen Kategorien enthalten. Daneben sind im entsprechenden Einzelfall weitere „angemessene Geheimhaltungsmaßnahmen" möglich oder gar erforderlich (siehe III. 2. a)).

a) Kategorisierung der Informationen nach ihrer Schutzwürdigkeit

Die zu schützenden Informationen sind entsprechend ihres Wertes für das Unternehmen bzw. ihrer Schutzwürdigkeit zu kategorisieren.[27] In die Beurteilung der Wichtigkeit und Schutzwürdigkeit der Informationen sollten neben der tatsächlichen Bedeutung der Geheimhaltung des jeweiligen Geheimnisses für das Unternehmen auch der objektive Wert sowie die spezifischen Merkmale des Geheimnisses einfließen. Eben diese Kriterien spielen später eine Rolle bei der Beurteilung der „angemessenen Geheimhaltungsmaßnahmen". Dabei könnten die Informationen in drei (Haupt-)Kategorien unterteilt werden; mehrere Geschäftsgeheimnisse gleicher Schutzwürdigkeit können in einer Schutzkategorie zusammengefasst werden:[28]

1. „Kronjuwelen" (existenzielle Informationen des Unternehmens);
2. „wichtige Informationen" (Informationen, deren Verlust dauerhaften wirtschaftlichen Nachteil verursachen können);
3. „sensible Informationen" (sonstige Informationen, deren Bekanntwerden einen kurzfristigen wirtschaftlichen Nachteil verursachen können);

Es sollte allerdings vermieden werden, alle denkbaren Informationen als geheim einzustufen; zum einen könnte dies bereits die Angemessenheit der Maßnahmen hindern und zum anderen den unternehmensinternen Geheimnisschutz verwässern.[29]

b) Festlegung „angemessener Geheimhaltungsmaßnahmen"

Da die Angemessenheit der Maßnahme nur am Einzelfall zu bestimmen ist und von verschiedenen Kriterien (siehe II. 1. c)) abhängt, müssen nicht uneingeschränkt die wichtigsten Informationen auch am besten geschützt sein. Das Schutzsystem ist auf die speziellen Risiken des Unternehmens abzustimmen. Sofern das Unternehmen etwa eine hohe Fluktuation auf Arbeitnehmerseite verzeichnet, sollte dies durch entsprechende arbeitsvertragliche Maßnahmen und häufige Schulungen des neuen Personals aufgefangen werden.[30] Ein Unternehmen mit häufigem Kundenkontakt dürfte hingegen das Augenmerk eher darauf zu richten haben, die tatsächliche Kenntnisnahme Dritter vom Geschäftsgeheimnis zu vermeiden. IT-Unternehmen mit nur wenig Personal sollten sich demgegenüber auf die digitale Informationssicherheit konzentrieren. Dies gilt insbesondere, wenn Informationen zwar als existenziell wichtig zu bewerten sind, sie allerdings keinen entsprechend strengen Sicherheitsanforderungen unterworfen werden können, weil ansonsten der Betriebsablauf erheblich gestört oder gar zum Erliegen gebracht würde.[31]

In der Regel dürften allerdings mit steigender Wichtigkeit der Informationen auch erhöhte Anforderungen an die durchzuführenden „angemessenen Geheimhaltungsmaßnahmen" zu stellen sein. Das Ri-

26 So bereits zur Know-how-Richtlinie *Baranowski/Glaßl*, BB 2016, 2563, 2568; *Maaßen*, GRUR 2019, 352, 356 f.; ähnlich auch *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 144.
27 *Maaßen*, GRUR 2019, 352, 356; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 144.
28 *Maaßen*, GRUR 2019, 352, 356; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 144; *Dann/Markgraf*, NJW 2019, 1774, 1776.
29 *Maaßen*, GRUR 2019, 352, 356.
30 Zur Know-how-Richtlinie bereits *Baranowski/Glaßl*, BB 2016, 2563, 2568.
31 *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 144.

siko zu geringer Schutzvorkehrungen liegt bei den Unternehmen und die Geschäftsleitung trägt die Verantwortung für die richtige Abwägung. Bei der Ausarbeitung des Schutzsystems und der Wahl der Schutzmaßnahmen sollte eng mit den jeweils betroffenen unternehmensinternen Abteilungen (bspw. Personalabteilung, R&D, IT, Compliance etc.) zusammengearbeitet werden, um Synergieeffekte zu bilden.[32] Die einzelnen Geheimhaltungsmaßnahmen lassen sich in verschiedene Kategorien einteilen:[33]

(1) Unternehmensbezogene organisatorische Maßnahmen:
- unternehmensinterne Vorgaben bezüglich des Umgangs mit vertraulichen Informationen (bspw. „Clear Desk Policy"), Festlegen eines Verantwortlichen für den Geheimnisschutz (Geheimnisschutzbeauftragter);[34]
- Kennzeichnung sensibler Informationen;[35]
- Zugang zur Informationen begrenzen und dokumentieren/Zugang ausschließlich auf „Need-to-know"-Basis;[36]
- „Travel Policy" bei Geschäftsreisen in Länder, in denen der Zoll auch digitale Inhalte mitgeführter Geräte kontrollieren kann;[37]- kein Outsourcing von Datenverarbeitung, oder nur unter strengen Auflagen/besonderer Schutz beim Transport von Geschäftsgeheimnissen außerhalb des Unternehmens.[38]

(2) Unternehmensbezogene faktische und technische Maßnahmen:
- technische Überwachung (bspw. Videokameras und Alarmanlagen) sowie Einrichtung von Zutrittskontrollanlagen und besonders abgeschirmten Bereichen (ggf. Sicherung von „Kronjuwelen" in Tresoren oder besonders gesicherten Räumen);[39]
- Besuchermanagement (bspw. externe Besucher nur in abgesonderten Bereichen)/Werksausweise (ggf. mit abgestufter Zugangsberechtigung) und Zugangskontrollen/Besucher verpflichten, eigene Aufzeichnungsgeräte (z. B. Handy) abzugeben;[40]
- Beschränkung des Computerzugriffs (bspw. personalisierte Nutzerkennung mit Passwortschutz, kein USB-Zugriff und/oder nur eingeschränkter Zugriff auf das Internet), Schutz gegen Cyber- und Hackerattacken nach aktuellem Stand der Technik (z. B. Firewalls und Virenschutz);[41]
- Einführung einer Sicherungs- und Verschlüsselungstechnik;[42]
- Verbot oder Beschränkung dienstlicher Nutzung privater Hardware, Mitnahme von Unterlagen und Verwendung eines unternehmenseigenen Computers im Rahmen des Home-Office;[43]
- Verbot oder Beschränkung der Benutzung dienstlicher Hardware für private Zwecke;- Vermeiden von „Cloud-Computing" (jedenfalls mit Serverstandort im außereuropäischen Ausland).[44]

(3) Organisatorische und vertragliche Maßnahmen gegenüber Mitarbeitern:
- hohe Sorgfaltsanforderungen bei der Einstellung von Personen, die Zugang zu Geschäftsgeheimnissen erhalten;[45]
- regelmäßige Schulungen bzw. Belehrungen der Personen, die Zugang zu Geschäftsgeheimnissen haben, zum Umgang mit vertraulichen Informationen;[46]
- Überwachung (z. B. im Hinblick auf Auffälligkeiten wie Aufruf und Versand bestimmter Daten, Zugriffsversuche in sensiblen Bereichen und Schwankungen im Datenvolumen; ggf. Mitbestimmungspflicht des Betriebsrats § 87 Abs. 1 Nr. 6 BetrVG);[47]
- „Exit-Interviews" vor dem Ausscheiden von Mitarbeitern, um festzustellen, zu welchen Informationen der Mitarbeiter Zugang hatte, sowie um die Herausgabe aller Daten, Dokumente und Geräte zu kontrollieren;[48]
- Regelung des Umgangs mit Geschäftsgeheimnissen in der täglichen Arbeit (z. B. Verlassen des Arbeitsplatzes nur nach Sperrung des Bildschirms, Informationen verschließen oder mit Passwort sichern, ein generelles Verbot der Weitergabe von Geschäftsgeheimnissen);[49]
- Vertraulichkeitsvereinbarungen (ggf. mit Vertragsstrafe) bezüglich bestimmter, klar definierter Geschäftsgeheimnisse (kein Verbot der Offenlegung gegenüber Arbeitnehmervertretern, § 3 Abs. 1 Nr. 3 GeschGehG) und bezüglich aller Geschäftsgeheimnisse mit der Klarstellung, dass die Arbeitnehmer hierdurch nicht in ihrer beruflichen Zukunft unzumutbar eingeschränkt werden (pauschale „Catch-All"-Klauseln sind keine „angemessenen Geheimhaltungsmaßnahmen");[50]
- nachvertragliches Wettbewerbsverbot (eine „Catch-All"-Klausel kann hier eine „angemessene Geheimhaltungsmaßnahmen" darstellen, muss allerdings auf zwei Jahre beschränkt werden und eine Entschädigung vorsehen).[51]

(4) Vertragliche Maßnahmen gegenüber Geschäftspartnern/Dritten:
- Vertraulichkeitsvereinbarungen, wobei die Geschäftsgeheimnisse so genau wie möglich bezeichnet werden sollten (schon aus Gründen der Vorsicht bei jeder Überlassung eines Geschäftsgeheimnisses ratsam, weil eine unterlassene Vertraulichkeitsvereinbarung Indizwirkung dafür entfalten könnte, dass der Geheimnisinhaber elementare Schutzmaßnahmen unterlässt);[52]
- vertragliche Pflichten, wem und wie der Geschäftspartner seinerseits Zugang zu Geschäftsgeheimnissen erteilen darf (insb. Verpflichtung, Dritten die gleichen Vertraulichkeitspflichten aufzuerlegen, denen der Geschäftspartner selbst unterliegt);[53]

32 Vgl. zur Know-how Richtlinie bereits *Baranowski/Glaßl*, BB 2016, 2563, 2568.
33 Die nachfolgende Liste erhebt dabei keinen Anspruch auf Vollständigkeit sondern stellt vielmehr exemplarisch mögliche Maßnahmen dar.
34 *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 144; *Maaßen*, GRUR 2019, 352, 359; *Dann/Markgraf*, NJW 2019, 1774, 1776; zur Know-how-Richtlinie bereits *Gregor*, ZCG 2016, 262, 265.
35 Ausweislich der Regierungsbegründung ist eine Kennzeichnung nicht erforderlich, wird aber dennoch empfohlen, vgl. *Maaßen*, GRUR 2019, 352, 358, und *Ohly*, GRUR 2019, 441, 444; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; Zur Know-how-Richtlinie bereits *Gregor*, ZCG 2016, 262, 265.
36 *Ohly*, GRUR 2019, 441, 444; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 144 f.
37 Zur Know-how Richtlinie bereits *Baranowski/Glaßl*, BB 2016, 2563, 2569.
38 *Maaßen*, GRUR 2019, 352, 358; zur Know-how-Richtlinie bereits *Brammsen*, ZIP 2016, 2193, 2197.
39 *Maaßen*, GRUR 2019, 352, 357; *Dann/Markgraf*, NJW 2019, 1774, 1776; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; zur Know-how-Richtlinie bereits *Gregor*, ZCG 2016, 262, 267.
40 *Maaßen*, GRUR 2019, 352, 357 f.; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; Zur Know-how-Richtlinie bereits *Heinzke*, ZCG 2016, 262, 182, und *Gregor*, ZCG 2016, 262, 267.
41 *Maaßen*, GRUR 2019, 352, 357; *Dann/Markgraf*, NJW 2019, 1774, 1776; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; *Baranowski/Glaßl*, BB 2016, 2563, 2569.
42 *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; zur Know-how-Richtlinie bereits *Brammsen*, ZIP 2016, 2193, 2198.
43 *Maaßen*, GRUR 2019, 352, 358; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; zur Know-how-Richtlinie bereits *Brammsen*, ZIP 2016, 2193, 2197.
44 Zur Know-how-Richtlinie bereits *Brammsen*, ZIP 2016, 2193, 2197.
45 *Maaßen*, GRUR 2019, 352, 359.
46 *Maaßen*, GRUR 2019, 352, 359; *Dann/Markgraf*, NJW 2019, 1774, 1776; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; zur Know-how-Richtlinie bereits *Gregor*, ZCG 2016, 262, 266.
47 *Maaßen*, GRUR 2019, 352, 359.
48 Zur Know-how-Richtlinie bereits *Gregor*, ZCG 2016, 262, 266.
49 *Maaßen*, GRUR 2019, 352, 357 f.
50 *Maaßen*, GRUR 2019, 352, 359; *Dann/Markgraf*, NJW 2019, 1774, 1776; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; *von Steinau-Steinrück*, NJW-Spezial 2019, 498, 498 f.; zur Know-how-Richtlinie bereits *Gregor*, ZCG 2016, 262, 266.
51 Zur Know-how Richtlinie bereits *Gregor*, ZCG 2016, 262, 266.
52 *Maaßen*, GRUR 2019, 352, 360; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; zur Know-how-Richtlinie bereits *Baranowski/Glaßl*, BB 2016, 2563, 2568.
53 Zur Know-how-Richtlinie bereits *Gregor*, ZCG 2016, 262, 266.

– ausdrücklicher vertraglicher Ausschluss des „Reverse Engineering“ (siehe III. 2. c));
– Vertraulichkeitsvereinbarungen mit unternehmensfremden Dritten, die auf zu schützende Informationen Zugriff haben (z. B. IT-Spezialisten, Handwerker, Reinigungspersonal).[54]

c) Insbesondere Vertraulichkeitsvereinbarungen und Vorbeugung von Reverse Engineering

Vergleichbar zur aktuell gängigen Praxis sollte weiterhin die Verwendung von *Vertraulichkeitsvereinbarungen* eine grundlegende Schutzmaßnahme für Geschäftsgeheimnisse sein.[55] Auf diese sollte – anders als bislang teilweise möglich – auch nicht mehr in bestimmten Situationen verzichtet werden, anderenfalls droht der Schutzverlust.[56] Im Rahmen dieser Vereinbarung kann auch nicht mehr nur auf einen (vermuteten) Geheimhaltungswillen abgestellt werden. Die Geschäftsgeheimnisse sollten in einer Vereinbarung konkret bezeichnet werden.[57] Dabei genügen auch hier die „Catch-All“-Klauseln nicht den Anforderungen an die Bestimmtheit.[58] Die Anforderungen an die Qualität von Vertraulichkeitsvereinbarungen werden damit künftig noch steigen. Es ist davon abzuraten, bereits vorhandene Muster statisch und ohne Anpassung zu verwenden.

Das nach § 3 Abs. 1 Nr. 2 GeschGehG grundsätzlich zulässige „Reverse Engineering“ sollte dabei möglichst vertraglich ausgeschlossen werden. Ein solcher Ausschluss ist nach allgemeiner Meinung der bisherigen juristischen Literatur zu diesem Thema auch zulässig.[59] Dafür spricht insbesondere der Wortlaut, wonach der Untersuchende „*keiner Pflicht zur Beschränkung der Erlangung*“ unterliegt. Ein vertragliches Verbot des Reverse Engineering stellt eine solche Pflicht zur Beschränkung dar. Um das Reverse Engineering möglichst zu erschweren, sollte darüber hinaus auch die Weitergabe des überlassenen Produkts an weitere Personen vertraglich untersagt werden. Eine den entsprechenden Standards genügende Vertraulichkeitsvereinbarung gewinnt damit erheblich an Bedeutung.

Generell sollten die Vertragspartner verpflichtet werden, Dritten die gleichen Vertraulichkeitspflichten aufzuerlegen, denen der Geschäftspartner selbst unterliegt. Das Unternehmen sollte stets darauf achten, „Herr seiner Geheimnisse“ zu sein.

3. Umfangreiche Dokumentation sowie regelmäßige Evaluation und Anpassung der angemessenen Geheimhaltungsmaßnahmen

Außerdem sollte eine konsequente und dauerhafte Umsetzung der „angemessenen Geheimhaltungsmaßnahmen“ ernst genommen werden. Die Ansprüche des Geschäftsgeheimnisschutzgesetzes können nur erfolgversprechend geltend gemacht werden, wenn es sich auch um Geschäftsgeheimnisse handelt, also um Informationen, die Gegenstand von „angemessenen Geheimhaltungsmaßnahmen“ sind. Hierfür tragen die Unternehmen die Beweislast, insbesondere dafür, dass Maßnahmen nicht nur auf dem Papier existierten, sondern auch tatsächlich umgesetzt wurden.[60]

Der Geheimnisinhaber muss daher im Zweifel beweisen, dass der Geheimnisschutz auch in der täglichen Arbeit gelebt wird.[61] Soweit sie nicht umgesetzt werden, handelt es sich auch nicht mehr um „angemessene Geheimhaltungsmaßnahmen“, sodass die Information kein Geschäftsgeheimnis ist und aus dem Anwendungsbereich des Geschäftsgeheimnisschutzgesetzes fällt.[62]

Unternehmen sollten daher jederzeit in der Lage sein, auch die praktische Anwendung des Geheimnisschutzkonzepts nachzuweisen. Sie sind gut beraten, die Charakteristika einzelner Geschäftsgeheimnisse (im Rahmen der Auflistung und Bewertung) sowie die Durchführung von Geheimhaltungsmaßnahmen ausreichend zu dokumentieren, regelmäßig zu evaluieren und ggf. anzupassen, um bereits im Vorfeld den Weg erfolgreicher gerichtlicher (Abwehr-)Maßnahmen zu ebnen.

IV. Fazit

Die Anforderungen an einen effektiven Geheimnisschutz sind gestiegen. Mit dem Erfordernis „angemessener Geheimhaltungsmaßnahmen“ sind Unternehmen, die ihr umfangreiches Know-how außerhalb von Patenten und Marken schützen wollen, nunmehr angehalten, im Rahmen ihres Compliance Systems ein Geheimnisschutzkonzept zu entwickeln, zu implementieren und dessen Umsetzung zu dokumentieren. Eine kontinuierliche Überwachung und Weiterentwicklung ist dabei ebenfalls notwendig. Synergieeffekte mit bestehenden Systemen wie dem Datenschutz und der IT-Sicherheit können und sollten genutzt werden. Die gängigen Vertraulichkeitsvereinbarungen sollten nicht mehr unbesehen statisch verwendet, sondern auf den Einzelfall angepasst werden. Andernfalls drohen auch wegen des nunmehr zulässigen „Reverse Engineerings“ erhebliche Schutzlücken. Für die Praxis bedeutet das: Unternehmen müssen *aktiv* angemessene Geheimhaltungsmaßnahmen implementieren, um weiterhin den Schutz ihrer Geschäftsgeheimnisse sicherzustellen.

Ingrid Burghardt-Richter, RAin/FAinHaGesR, ist Partnerin der FPS Fritze Wicke Seelig Partnerschaftsgesellschaft von Rechtsanwälten mbB in Düsseldorf. Sie berät Unternehmer und Unternehmen bei gesellschaftsrechtlichen Gestaltungen, insbesondere im Bereich von Übernahmen und Beteiligungen. Zudem berät sie in- und ausländische Mandanten bei der konzeptionellen Gestaltung unternehmerischer Kooperationen.

Dr. Johannes Bode ist Rechtsanwalt bei FPS Fritze Wicke Seelig Partnerschaftsgesellschaft von Rechtsanwälten mbB in Düsseldorf. Seine Tätigkeitsschwerpunkte umfassen in handels- und gesellschaftsrechtlicher Hinsicht die Beratung bei Gründung einer Gesellschaft, bei der Gestaltung von Gesellschaftsverträgen, bei Gesellschafterwechseln und Umwandlungen sowie der Betreuung im Tagesgeschäft. Darüber hinaus berät er im Handels- und Vertragsrecht bei Vertragsgestaltungen und Verhandlungen.

54 *Maaßen*, GRUR 2019, 352, 360.
55 Vgl. *Maaßen*, GRUR 2019, 352, 360; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145; *Heinzke*, ZCG 2016, 262, 181 ff.
56 *Heinzke*, ZCG 2016, 262, 182 f.
57 *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145.
58 *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145.
59 *Dann/Markgraf*, NJW 2019, 1774, 1776; *Voigt/Herrmann/Grabenschröer*, BB 2019, 142, 145 f.; *Ohly*, GRUR 2019, 441, 447; kritisch hinsichtlich eines zeitlich unbegrenzt geltenden Ausschlusses *Rath/Schreiner/Laoutoumai*, Erste Hilfe zum Geschäftsgeheimnisschutzgesetz (GeschGehG), 2019, S. 22.
60 BT-Drs. 19/4724, 24; *Maaßen*, GRUR 2019, 352, 360; *Lamy/Vollprecht*, IR 2019, 201, 203.
61 *Maaßen*, GRUR 2019, 352, 360.
62 *Maaßen*, GRUR 2019, 352, 360.