www.betriebs-berater.de

Betriebs Berater

70 Jahre

43 | 2016

Recht | Wirtschaft | Steuern

24.10.2016 | 71. Jg.
Seiten 2561–2624

BB-Rechtsprechungsreport zu bilanziellen Aspekten des Umwandlungssteuerrechts 2015/2016

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Anne Baranowski, LL.M., RAin, und Ramón Glaßl, LL.M., RA

Anforderungen an den Geheimnisschutz nach der neuen EU-Richtlinie

Vor Inkrafttreten der „Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtwidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung" (Richtlinie 2016/943) („Richtlinie") waren Geschäftsgeheimnisse im europäischen Binnenmarkt nicht gleichermaßen geschützt. Aus diesen Gründen hat sich die Europäische Kommission im Rahmen der Strategie „Europa 2000" zum Ziel gesetzt, den Schutz von Geschäftsgeheimnissen zu harmonisieren. Die Richtlinie soll insbesondere Anreize zu grenzüberschreitendem Know-how-Austausch fördern und zugleich Wettbewerbsvorteile der Mitgliedstaaten gegenüber außereuropäischer Konkurrenz sichern. Welche Anforderungen an den Know-how-Schutz als Bestandteil der unternehmerischen Compliance nach der neuen EU-Richtlinie zu stellen sind, ist Gegenstand des Beitrags.

I. Einleitung

Zwar gibt die Definition in Art. 39 Abs. 2 TRIPS auf internationaler Ebene einen Mindeststandard für den Schutz von Geschäftsgeheimnissen vor, der von den Mitgliedstaaten und der Europäischen Union selbst zu beachten ist. Gleichwohl hat sich europaweit bislang kein einheitliches Verständnis zum Geheimnisschutz gebildet. Der Geheimnisschutz erfolgt teilweise im Straf-, Kartell- oder Wettbewerbsrecht, zumeist nicht jedoch über das Zivilrecht. Die uneinheitlichen und intransparenten Regelungen zum Schutz von Geschäftsgeheimnissen beeinträchtigen die Unternehmen, sich effizient gegen die Angriffe auf ihr Know-how zu wehren. Zudem drohen schützenswerte Informationen bei der Übertragung in einen Mitgliedstaat mit niedrigerem Schutzniveau entwertet zu werden (COM (2013) 813, final, S. 6). Aufgrund des uneinheitlichen Schutzniveaus von Geschäftsgeheimnissen in den einzelnen Mitgliedstaaten wird der freie Warenverkehr, Innovation und Wettbewerbsfähigkeit der europäischen Unternehmen behindert. Der mangelnde Schutz gefährdet die auf Geschäftsgeheimnissen basierenden Wettbewerbsvorteile. Schon die einmalige Verletzung bzw. das Offenkundigwerden von Geschäftsgeheimnissen kann zu deren Entwertung führen, sodass damit auch der Wissensvorsprung im Wettbewerb sowie die Wettbewerbsfähigkeit verloren gehen.

II. Entstehung und Konzeption der Richtlinie

Im Jahr 2013 veröffentlichte die EU-Kommission den ersten Entwurf einer Richtlinie, im Mai 2014 verabschiedete der EU-Rat die erste konsolidierte Fassung und im Juni 2015 veröffentlichte das Europäische Parlament einen Bericht über den Richtlinien-Entwurf, auf dessen Grundlage die informellen Trilog-Verhandlungen zwischen EU-Parlament, Rat und Kommission stattfanden. Die nach Abschluss der Trilog-Verhandlungen entstandene Version der Richtlinie wurde vom EU-Parlament angenommen und ist am 5.7.2016 in Kraft getreten. Im Folgenden wird untersucht, inwieweit die Richtlinie den Geheimnisschutz im deutschen Recht beeinflusst.

Die Richtlinie bietet eine rechtliche Grundlage für den Erwerb, die Nutzung und Offenlegung von Geschäftsgeheimnissen innerhalb der Europäischen Union. Sie betrifft im Wesentlichen drei zentrale Regelungsbereiche.[1] Zunächst wird erstmals innerhalb der Union der nicht harmonisch verwendete Begriff des „Geschäftsgeheimnisses" definiert.[2] Des Weiteren wird der Umfang der zulässigen Nutzung mit Geschäftsgeheimnissen festgelegt. Im Übrigen werden im Verfahrensrecht Maßnahmen eingeführt, die dem Schutz von Geschäftsgeheimnissen im Gerichtsverfahren dienen sollen. Mit der Richtlinie wird jedoch keine Vollharmonisierung angestrebt, sodass die Mitgliedstaaten ergänzende Vorschriften vorsehen können. Die Richtlinie ist bis zum 9.6.2018 ins nationale Recht umzusetzen.

III. Status quo des Geheimnisschutzes im deutschen Recht

Im deutschen Recht gibt es keine gesetzliche Definition für Geschäftsgeheimnisse. Die maßgeblichen Bestimmungen zum Schutz von Geschäftsgeheimnissen sind vielmehr über verschiedene Rechtsgebiete und Normen verteilt. Der Umgang mit Geschäftsgeheimnissen richtet sich im deutschen Recht jedoch vornehmlich nach § 17 UWG sowie nach dem lauterkeitsrechtlichen Nebenstrafrecht. Die Offenbarung von geheimen Informationen wird verfolgt beim Geheimnisverrat durch Beschäftigte nach § 17 Abs. 1 UWG, bei der Betriebsspionage nach § 17 Abs. 2 Nr. 1 UWG und bei der Geheimnishehlerei nach § 17 Abs. 2 Nr. 2 UWG. Bei § 17 UWG handelt es sich systematisch um eine Strafvorschrift, die jedoch eher das Unternehmen als die schutzbedürftigen Informationen selbst schützt. Erst der unlautere Eingriff in die Geheimnissphäre, zum Beispiel durch Verstoß gegen eine Geheimhaltungsverpflichtung, löst den Geheimnisschutz aus. Geschäftsgeheimnisse werden durch die Vorschriften des Wettbewerbsrechts zwar als vermögenswerte Positionen anerkannt, aber nicht als Eigentumsrecht oder eigentumsähnliches Recht ausgestaltet.[3] Ein Schutz gegen eine gutgläubige Verwendung geheimer Informationen besteht jedoch nicht. Damit unterscheidet sich der Geheimnisschutz von den Rechten am geistigen Eigentum, die auf einen Rechtsinhaber zugeschnitten sind und bei denen eine Schutzrechtsposition einem Rechtssubjekt als absolutes Recht zugeordnet.[4] Im deutschen Recht fehlt jedoch bislang die Anerkennung von Geschäftsgeheimnissen als absolute subjektive Rechte. Durch die Richtlinie kommt dem

1 *Koós*, MMR, 2016, 224, 225.
2 *Gaugenrieder*, BB, 2014, 1987.
3 *McGuire*, GRUR Int., 2010, 829, 831.
4 *Heinzke*, CCZ, 2016, 179.

Geheimnisschutz nun erstmals eine Art absolutes Recht zu, sodass damit Neuland betreten wird.

Im deutschen Recht sind nach der Rechtsprechung des BGH Geschäftsgeheimnisse Tatsachen oder Sachverhalte, die nicht offenkundig sind, d. h., die nur einem begrenzten Personenkreis bekannt sind und an deren Geheimhaltung ein berechtigtes Interesse der Gesellschaft besteht.[5] Das Geheimhaltungsinteresse der Gesellschaft wird in erster Linie objektiv bestimmt. Danach ist dasjenige geheimhaltungsbedürftig, was ein unbefangener Beobachter nach dem Gesamterscheinungsbild der Gesellschaft und ihres Geschäfts für geheimhaltungsbedürftig halten darf, insbesondere wenn durch die Offenbarung der Tatsachen ein materieller oder immaterieller Schaden drohen könnte[6] oder wenn die Gesellschaft zur Geheimhaltung kraft Gesetz (z. B. Datenschutz) oder Vereinbarung verpflichtet ist. Soweit ein objektives Geheimhaltungsinteresse besteht, kommt es auf den Geheimhaltungswillen der Gesellschaft nicht an.[7] Ein subjektiver Geheimhaltungswille ist also nicht erforderlich.[8]

Betriebs- und Geschäftsgeheimnisse sind im Gesetz nicht definiert, allerdings ist deren Schutz seit jeher anerkannt.[9] Sie werden maßgeblich durch Rechtsprechung bestimmt. Betriebsgeheimnisse sind Geheimnisse, die sich auf die Erreichung des Geschäftszwecks beziehen.[10] Sie liegen in der Regel auf technischem Gebiet und betreffen zum Beispiel Fabrikationsverfahren, Maschinen, Konstruktionspläne und technische Geräte. Geschäftsgeheimnisse betreffen dagegen Tatsachen und Erkenntnisse von wirtschaftlicher Bedeutung.[11] Es sind solche Geheimnisse, die sich auf das Know-how eines Unternehmens beziehen, wie zum Beispiel Kundenlisten, Jahresabschlüsse, Preisberechnungen, Vertragsabschlüsse. In der Praxis ist eine Differenzierung zwischen Betriebs- und Geschäftsgeheimnis weder rechtlich geboten noch aus sonstigen Gründen erforderlich. Die Voraussetzungen und Rechtsfolgen beider Begriffe decken sich in der Regel.[12]

Ergänzend erfahren Informationen Schutz durch arbeits- und gesellschaftsrechtliche Bestimmungen sowie durch Sondergesetze wie zum Beispiel § 6 S. 2 IFG, § 140c Abs. 1 S. 3 PatG, § 138 TKG, § 203 StGB und § 85 GmbHG.

IV. Geheimnisschutz nach der Richtlinie

Nach der Richtlinie werden die Mitgliedstaaten verpflichtet, einen zivilrechtlichen Geheimnisschutz vorzusehen (Art. 6 Abs. 1 Richtlinie). Ein Schritt zur Harmonisierung des Schutzes von Geschäftsgeheimnissen ist vor allem die Definition des Begriffs „Geschäftsgeheimnis" sowie die Festlegung von Situationen, in denen der Erwerb, die Nutzung und/oder die Offenlegung von Geschäftsgeheimnissen zulässig sein soll (vgl. Erwägungsgrund 4 der Richtlinie).

1. Definition Geschäftsgeheimnis

Das Geschäftsgeheimnis wird in Art. 1 Abs. 1 Richtlinie definiert und einem Rechtsträger zugeordnet. Inhaber des Geschäftsgeheimnisses ist die Person, die die rechtmäßige Kontrolle über das Geschäftsgeheimnis hat. Dabei orientiert sich die Richtlinie an der Regelungssystematik des geistigen Eigentumsrechts. Das Schutzrecht wird festgelegt und durch eine Zuordnungsnorm dem Träger zugewiesen.[13] Ein Ausschließlichkeitsrecht für Geheimnisse wird durch die Richtlinie jedoch nicht geschaffen.[14] Zwar wird der Geheimnisschutz ähnlich wie ein geistiges Eigentumsrecht geformt, bleibt jedoch dahinter zurück. Nach der Konzeption der Richtlinie ist der rechtliche Schutz der Geschäftsgeheimnisse weiterhin nur als Zugangsschutz konzipiert. Ansprüche bestehen daher gegen denjenigen, der in die vom Geheimnisträger errichtete Schutzsphäre eindringt oder gegen den bösgläubigen Dritten, der die Geschäftsgeheimnisse unmittelbar oder mittelbar vom Ersttäter erlangt hat.[15]

Die Richtlinie sieht in Art. 2 Nr. 1 eine sich an Art. 39 Abs. 2 des TRIPS-Übereinkommens orientierende Definition von Geschäftsgeheimnissen vor. Danach sind als Geschäftsgeheimnis die Informationen anzusehen, die geheim sind, deshalb einen kommerziellen Wert besitzen und Gegenstand angemessener Geheimhaltungsmaßnahmen sind. Der so bestimmte Schutzgegenstand entspricht im Wesentlichen der von der deutschen Rechtsprechung entwickelten Definition des Geschäftsgeheimnisses, ist jedoch nicht mit ihr identisch.

Künftig müssen also konkrete faktische und rechtliche Geheimhaltungsmaßnahmen ergriffen werden, um Geheimnisschutz zu erlangen. Daraus folgt konkreter Handlungsbedarf für die Unternehmen, insbesondere an der Schnittstelle zwischen Informationsmanagement und Compliance (s. hierzu IV. 4. und insbes. VIII.).

Der Erwägungsgrund 14 der Richtlinie stellt zudem klar, dass von der Definition auch Know-how, technologische Informationen und Geschäftsinformationen umfasst sein sollen.

2. Geheime Information

Geheimnisschutz wird nur für Informationen gewährt, die weder in ihrer Gesamtheit noch in der genauen Zuordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Information umgehen, allgemein bekannt oder ohne Weiteres zugänglich sind, Art. 2a der Richtlinie. Diese Definition entspricht dem von der deutschen Rechtsprechung entwickelten Merkmal der fehlenden Offenkundigkeit. Hiernach darf die Information nur einem begrenzten Personenkreis bekannt sein. Informationen, die von interessierten Fachkreisen ohne größere Schwierigkeiten in Erfahrung gebracht werden können, sind jedoch nicht geschützt.[16] Der Geheimnisschutz bleibt jedoch gewahrt, wenn die Information anderen zur Vertraulichkeit verpflichteten Personen mitgeteilt wird. Entscheidend ist dabei, dass der Geheimnisinhaber die Kontrolle über diesen Personenkreis behält. Sobald die Information jedoch auf lauterem Weg im relevanten Fachkreis bekannt wird, entfällt der Schutz. Nach bisherigem Recht ist zwar jede unautorisierte Weitergabe potentiell geheimnisschädlich, allerdings erlischt der Schutz erst ab einem gewissen Verbreitungsgrad.[17] Dies sollte sich durch die Richtlinie nicht ändern. Geheimnisschädlich ist nach der

5 BGH, 20.5.1996 – II ZR 190/95, BB 1996, 1627, NJW 1996, 2576.
6 BGH, 20.5.1996 – II ZR 190/95, BB 1996, 1627, NJW 1996, 2576.
7 BGH, 20.5.1996 – II ZR 190/95, BB 1996, 1627, NJW 1996, 2576; *Haas*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 85, Rn. 10.
8 *Haas*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 85, Rn. 10.
9 *Schoch*, in: Informationsfreiheitsgesetz, 2. Aufl. 2016, § 6, Rn. 14.
10 Vgl. BGH, 7.11.2002 – I ZR 64/00, NJW 2003, 618, 620 – Präzisionsmessgeräte; LAG Köln, 18.12.1987 – 2 Sa 623/84, Fundheft für Arbeits- und Sozialrecht (FHArbSozR) 34 Nr. 1577; *Ohly*, in: Ohly/Sosnitza, UWG, 7. Aufl. 2016, § 17, Rn. 5; *Richardi*, in: Richardi, BetrVG, 15. Aufl. 2016, § 79, Rn. 5.
11 Vgl. BVerfG, 14.3.2006 –1 BvR 2087/03, NVwZ 2006, 1041–1048, Rn. 87 – Deutsche Telekom; BGH, 19.12.2002 – I ZR 119/00, BB 2003, 760 Ls, NJW-RR 2003, 833–834, 833 – Verwertung von Kundenlisten; AP BetrVG 1972 § 79 Nr. 2, BeckRS 9998, 149818; *Richardi*, in: Richardi, BetrVG, 15. Aufl. 2016, § 79, Rn. 5.
12 *Löwisch*, in: Ebenroth u. a., Handelsgesetzbuch, 3. Aufl. 2014, § 90, Rn. 2.
13 *Heinzke*, CCZ, 2016, 179, 180.
14 COM (2013) 813 final, 16. Erwägungsgrund.
15 *Heinzke*, CCZ, 2016, 179, 180.
16 *Heinzke*, CCZ, 2016, 179, 181.
17 *Köhler*, in: Köhler/Bornkamm, UWG, 34. Aufl. 2016, § 17, Rn. 7a.

Richtlinie erst die Bekanntheit oder leichte Zugänglichkeit der Informationen in den maßgeblichen Fachkreisen.[18]

3. Kommerzieller Wert

Von der Richtlinie sind nur solche Informationen geschützt, die einen kommerziellen Wert haben. Dieses Kriterium entspricht den von der deutschen Rechtsprechung ausgestalteten Begriffen der Betriebsbezogenheit sowie dem Geheimhaltungsinteresse.[19] Nach diesen Kriterien sind bislang nur solche Informationen geschützt, die mit der Geschäftstätigkeit des Geheimnisinhabers in Beziehung stehen und an deren Geheimhaltung ein berechtigtes wirtschaftliches Interesse besteht. Ein berechtigtes wirtschaftliches Interesse soll immer dann gegeben sein, wenn die Information für die Geschäftsfähigkeit des Geheimnisinhabers von Bedeutung ist. Eine bestimmte Wertschwelle wird nicht verlangt. Schutzfähig bleiben alle irgendwie kommerziell verwertbaren Informationen.[20]

4. Angemessene Geheimhaltungsmaßnahmen

Informationen müssen Gegenstand von den Umständen entsprechenden Geheimhaltungsmaßnahmen sein, Art. 1 c der Richtlinie. Für das Kriterium der angemessenen Geheimhaltungsmaßnahmen gibt es im deutschen Recht bisher keine Entsprechung.[21] Das Kriterium der „angemessenen Geheimhaltungsmaßnahmen" stellt im Vergleich zur bisherigen deutschen Rechtslage eine Verschlechterung dar, da ein rechtlicher Schutz nur bestehen soll, wenn die Geheimnisträger hinreichende Maßnahmen zum Schutz ihrer Geschäftsgeheimnisse darlegen und nachweisen können. Im deutschen Recht wird ein Geschäftsgeheimnis jedoch bereits dann angenommen, wenn geheime Tatsachen von kommerziellem Wert nach dem erkennbaren subjektiven Willen des Inhabers geheim gehalten werden sollen, wobei der Geheimhaltungswille vermutet wird.[22] Für alle innerbetrieblichen Kenntnisse und Vorgänge wird im deutschen Recht vermutet, dass diese nach dem Willen des Betriebsinhabers geheim zu halten sind, ohne dass es dazu konkreter Maßnahmen bedarf.[23] Der Wille zur Geheimhaltung soll sich also schon aus der Natur der geheim zu haltenden Informationen ergeben.[24] Da den Mitgliedstaaten erlaubt ist, einen weitergehenden Schutz einzuräumen, und die Definition der Geschäftsgeheimnisse keine zwingende Vorgabe darstellt (vgl. Art. 1 Abs. 1 Richtlinie in Verbindung mit dem Erwägungsgrund 10), kann der deutsche Gesetzgeber bei der Umsetzung der Richtlinie die bisherige Definition hinsichtlich des Geheimhaltungswillen beibehalten.

Künftig müssen jedoch auf jeden Fall Geheimhaltungsmaßnahmen ergriffen werden, Art. 2c der Richtlinie. Die Richtlinie sieht zwar keinen Maßnahmenkatalog vor, allerdings müssen die Maßnahmen „angemessen" und „den Umständen entsprechend" sein. Je nach Art und Bedeutung der geheimen Information können sich Grad und Intensität der erforderlichen Sicherungsmaßnahmen im Einzelfall unterscheiden.[25] Schützenswerte Informationen müssen somit identifiziert und entsprechend ihrer Wichtigkeit mit einem abgestuften Schutzsystem gesichert werden. Je wichtiger die schützenswerte Information ist, desto umfassender müssen auch die erforderlichen Sicherheitsmaßnahmen ausfallen. Dazu gehören auch technische und organisatorische sowie rechtliche Maßnahmen. Zu geringe Schutzmaßnahmen können sich künftig als fatal erweisen. Gelingt es dem Geheimnisinhaber nicht, ergriffene Schutzmaßnahmen darzulegen und nachzuweisen oder sind die Schutzmaßnahmen nicht ausreichend, geht dies zu seinen Lasten. Dieses Risiko kann zum Beispiel durch geeignete Informationsschutzsysteme und Vertraulichkeitsvereinbarungen beschränkt werden.[26]

5. Erwerb von Geschäftsgeheimnissen

Geschützt ist der Inhaber von Geschäftsgeheimnissen vor dem rechtswidrigen Erwerb sowie der rechtswidrigen Nutzung und Offenlegung seiner Geschäftsgeheimnisse. Art. 3 der Richtlinie erklärt Vorgehensweisen, die unter den gegebenen Umständen „mit einer seriösen Geschäftspraxis vereinbar sind", für rechtmäßig. Verhaltensweisen, die nicht mit einer seriösen Geschäftspraxis vereinbar sind, werden durch Art. 4 der Richtlinie für rechtswidrig erklärt. Die maßgebliche Grenze zwischen Rechtmäßigkeit und Rechtswidrigkeit bildet somit der unbestimmte Rechtsbegriff der „seriösen Geschäftspraxis". Dieser Begriff ist sehr offen formuliert und wird durch die Rechtsprechung konkretisiert werden müssen. Diese Rechtsunsicherheit ist für die Praxis wenig hilfreich. Als seriöse Geschäftspraxis sieht Art. 3 Abs. 1b der Richtlinie ausdrücklich auch das sogenannte „Reverse Engineering" an. Ein Geschäftsgeheimnis kann demnach nicht nur durch unabhängige Entdeckung oder Schöpfung rechtmäßig erworben werden, sondern auch durch Untersuchung und Dekonstruktion eines rechtmäßig in den Verkehr gelangten Produkts, Art. 3 Abs. 1a und b der Richtlinie.

Rechtswidriger Erwerb, Nutzung und Offenlegung von Geschäftsgeheimnissen werden durch einen Katalog verbotener Handlungen (Art. 4 der Richtlinie) und Verbotsausnahmen (Art. 5 der Richtlinie) geregelt. Als rechtswidrig gilt der Erwerb, wenn er ohne die Zustimmung des Geheimnisinhabers durch unbefugten Zugang, unbefugte Aneignung oder unbefugtes Kopieren erfolgt, Art. 4 Abs. 2a der Richtlinie. Gegen derartige Handlungen sind alle körperlichen und unkörperlichen Manifestationen des Geschäftsgeheimnisses geschützt. Um eine autonome Auslegung der Richtlinie zu gewährleisten, wurden diese möglichen Tathandlungen nur generisch umschrieben. Parallel zum Auffangtatbestand für den rechtmäßigen Erwerb sieht die Rechtlinie somit auch einen sehr weit gefassten Auffangtatbestand für den rechtswidrigen Erwerb vor. Der Erwerb soll auch bei jedem sonstigen Verhalten, das mit einer seriösen Geschäftspraxis nicht vereinbar ist, rechtswidrig sein, Art. 4 Abs. 2b der Richtlinie.

Als rechtswidrig gelten die Nutzung und Offenlegung durch den Erstverletzer, der sich das Geschäftsgeheimnis zuvor selbst auf rechtswidrige Weise verschafft hat, Art. 4 Abs. 3a der Richtlinie. Einen gutgläubigen lastenfreien Erwerb von Geschäftsgeheimnissen kennt die Richtlinie jedoch nicht. Der Geheimnisinhaber kann sich allerdings gegen den später bösgläubig werdenden Zweiterwerber wehren. Wird der Erwerber später, zum Beispiel durch einen Hinweis des Geheimnisinhabers, bösgläubig und erfährt, dass er das Geschäftsgeheimnis von einer Mittelsperson erworben hat, der dieses rechtswidrig genutzt oder offengelegt hat, so nutzt er das Geschäftsgeheimnis ab diesem Zeitpunkt

18 *Heinzke*, CCZ, 2016, 179, 181.
19 *Heinzke*, CCZ, 2016, 179, 182.
20 *Heinzke*, CCZ, 2016, 179, 182; OLG Düsseldorf, 30.7.1998 – 2 U 162/97.
21 *Gärtner*, NZG, 2014, 650, 651.
22 *Gärtner/Schlüter*, in: Deutscher AnwaltSpiegel, Ausgabe 11 vom 1.6.2016, www.deutscher anwaltspiegel.de/wp-content/uploads/2016/06/DAS-Online_Ausgabe-11-2016.pdf (Abruf. 11.10.2016) S. 3–6, S. 4.
23 *Harte-Bavendamm*, in: Henning-Bodewig/Harte-Bavendamm, UWG, 2. Aufl. 2013, § 17, Rn. 5.
24 BGH, 4.9.2013 –5 StR 152/13, NStZ 2014, 325.
25 *Kalbfus/Harte-Bavendamm*, GRUR, 2014, 453.
26 *Heinzke*, CCZ, 2016, 179, 182.

rechtswidrig.[27] Bei Bösgläubigkeit gilt darüber hinaus auch das Herstellen, das Anbieten oder Inverkehrbringen bzw. der Import oder Export und die Lagerung von Produkten, die in erheblichem Umfang auf Geschäftsgeheimnissen basieren, als rechtswidrige Nutzung. Für den zunächst gutgläubigen Verletzer besteht unter Umständen die Möglichkeit, Ansprüche des Geheimnisinhabers im Verletzerprozess durch Zahlung einer Lizenzgebühr abzuwenden, Art. 13 Abs. 3 der Richtlinie.

V. Reverse Engineering

Wenn sich ein Konkurrent durch Entschlüsselung oder Dekonstruktion (auch Reverse Engineering genannt) von auf dem Markt frei erhältlichen Produkten Geschäfts- oder Betriebsgeheimnisse verschafft, kann dies den Tatbestand des derzeit geltenden § 17 Abs. 2 Nr. 1a UWG erfüllen. Hiernach wird ebenfalls bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel unbefugt verschafft oder sichert. Voraussetzung ist jedoch, dass die Information nur mit größeren Schwierigkeiten und Kosten in Erfahrung gebracht werden kann; ist dies der Fall, geht der Geheimnischarakter mit dem freien Erwerb nicht verloren.[28] Nach wohl herrschender Meinung ist Reverse Engineering damit grundsätzlich unzulässig.[29]

Insofern scheint das derzeit geltende deutsche Recht im Schutz vor Reverse Engineering weiter zu gehen als andere Rechtsordnungen, wie beispielsweise die der Vereinigten Staaten von Amerika. Diese lässt Reverse Engineering wegen seiner innovationsfördernden Funktion ausdrücklich zu, solange keine Rechte des Geistigen Eigentums verletzt werden.[30] Auch die Europäische Union sieht in der Richtlinie in Art. 3 Abs. 1b ausdrücklich vor, dass eine Erlangung von Informationen durch „*Beobachtung, Untersuchung, Rückbau oder Testen eines Produkts oder Gegenstands, das bzw. der öffentlich verfügbar gemacht wurde oder sich im rechtmäßigen Besitz des Erwerbers der Information befindet, der keiner rechtsgültigen Pflicht zur Beschränkung des Erwerbs des Geschäftsgeheimnisses unterliegt*“, rechtmäßig ist. Insofern ist eine Dekonstruktion – also das Reverse Engineering – ausdrücklich grundsätzlich zulässig. Insofern wird nunmehr auch innerhalb der Europäischen Union die Innovationsförderung als bedeutsamer als der Know-how-Schutz angesehen.[31] Nach Ansicht von Prof. *Dr. Mary- Rose McGuire* geht der Schutz auf europäischer Ebene jedoch weiter als auf deutscher Ebene, da zulässiges Reverse Engineering nicht als Schutzhindernis (wie im deutschen Recht), sondern als Schranke ausgestaltet ist.[32]

Ungeachtet dieser eher theoretischen Diskussion haben Unternehmen und Geheimnisträger jedoch die Möglichkeit, Reverse Engineering in gewissem Maße einzuschränken. Gemäß Art. 3 Abs. 1b der Richtlinie darf der Erwerber keiner rechtsgültigen Pflicht zur Beschränkung des Erwerbs des Geschäftsgeheimnisses unterliegen. Insofern ist Unternehmen die Möglichkeit an die Hand gegeben, beispielsweise in R&D-Verträgen ein entsprechendes vertragliches Verbot aufzunehmen.[33] Hier zeigt sich ein durch die gesamte Richtlinie ziehender roter Faden: Wird das Unternehmen nicht aktiv tätig, um seine Informationen zu schützen, wird ihm kein gesetzlicher Schutz gewährt.

Über diese Möglichkeiten hinaus sind Unternehmen auf den bestehenden Schutz aus gewerblichen Schutzrechten[34] (insbesondere Patente) beziehungsweise geistigem Eigentum[35] beschränkt und werden nur bei einer Verletzung auch dieser Rechte gegen das Reverse Engineering vorgehen können.

VI. Whistleblowing

Derzeit ist Geheimnisverrat als strafrechtliche Vorschrift ausgestaltet: Wer ein Geschäfts- oder Betriebsgeheimnis unbefugt mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, § 17 Abs. 1 UWG. Einzig die Ausgestaltung als Antragsdelikt sorgt dafür, dass nicht jeder Geheimnisverrat zugleich auch bei der Staatsanwaltschaft landet. Insofern stellt sich die Frage, wie mit Whistleblowern umzugehen ist; also Personen, die Geheimnisse bewusst verraten, um eine bestimmte Tatsache der „Öffentlichkeit“ bekannt zu machen.

Hier dürfte grundsätzlich zwischen zwei verschiedenen Sachverhalten zu unterscheiden sein: Zum einen wird als Whistleblower jemand angesehen, der Geheimnisse verrät, weil er sich moralisch hierzu verpflichtet fühlt. Dies dürfte beispielsweise dann der Fall sein, wenn ein Mitarbeiter strafrechtlich relevantes Verhalten eines Kollegen oder Vorgesetzten meldet. Aber auch der Verrat von Geheimnissen in großem Stile (siehe Wikileaks und *Edward Snowden*) dürfte hierunter fallen (hierzu unter Ziff. 1). Zum anderen gibt es denjenigen Whistleblower, der einen Sachverhalt des Geheimnisverrats aufdeckt, an dem er selbst beteiligt war; man könnte also quasi von einer Selbstanzeige sprechen (hierzu unter Ziff. 2).

1. Das klassische Whistleblowing

Die rechtliche Diskussion bei Whistleblowern spielt sich im Wesentlichen auf der Ebene der Rechtswidrigkeit der Tathandlung ab: War der Geheimnisverrat unbefugt, geschah er also unter Verstoß gegen dienstliche Verschwiegenheitspflichten oder ohne Rechtfertigungsgrund?[36] Für die Beantwortung dieser Frage ist insbesondere bedeutsam, ob es sich um internes oder externes Whistleblowing handelt.

Internes Whistleblowing ist der unternehmensinterne Verrat eines Geheimnisses zum Zwecke der Aufdeckung von Missständen, Vorgängen oder Straftaten; externes Whistleblowing ist letztlich die Strafanzeige.[37] Bislang galt der Grundsatz, dass internes Whistleblowing insbesondere dann ungerechtfertigt bzw. unbefugt sein soll, wenn das Unternehmen Kontroll- und Selbststeuerungssysteme installiert hat.[38] Bei externem Whistleblowing hingegen wird häufig differenzierter vorgegangen und darauf abgestellt, ob der Geheimnisverrat angemessen war oder ob nicht zuvor ein internes Whistleblowing hätte stattfinden müssen.[39]

27 *Heinzke*, CCZ, 2016, 179–183, 181.
28 *Köhler*, in Köhler/Bornkamm, UWG, 34. Aufl. 2016, § 17, Rn. 8; *Ohly*, in Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 7. Aufl. 2016, § 17, Rn. 26a.
29 RGZ 149, 329, 334; *Harte-Bavendamm*, in: Gloy/Loschelder/Erdmann, Wettbewerbsrecht, 4. Aufl. 2010, § 77, Rn. 14; *Ohly*, in: Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 7. Aufl. 2016, § 17, Rn. 26a; einschränkend wohl OLG Düsseldorf, 30.7.1998 – 2 U 162/97, OLGR 1999, 55, wonach Fortschritte im Reverse Engineering zu Lasten des Geheimnisträgers gehen sollen, siehe auch *Köhler*, in Köhler/Bornkamm, UWG, 34. Aufl. 2016, § 17, Rn. 8.
30 *Ohly*, in Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 7. Aufl. 2016, § 17, Rn. 26a m. w. N.
31 Eine ausführliche Analyse des Reverse Engineering mit einer gelungenen Auseinandersetzung mit diesem Phänomen ist zu finden bei *Harte-Bavendamm*, FS Köhler, 2014, S. 245 ff.
32 *McGuire*, Know-How & Reverse Engineering, Unterschiede zwischen dem Schutz de lege lata und der geplanten RL, GRUR Bezirksgruppe Frankfurt, Januar 2016, abrufbar unter www.jura.uni-osnabrueck.de/fileadmin/public/media/LS-McGuire/PDFs/V_2016_01_GRUR_Frankfurt_Know-how___RE_Pr%C3%A4sentation_MRM.pdf (Abruf: 29.9.2016).
33 S. auch Erwägungsgrund 16 der Richtlinie; *Heinzke*, CCZ 2016, 179, 180; so wohl auch schon OLG Düsseldorf, 30.7.1998 – 2 U 162/97, OLGR 1999, 55.
34 S. insbesondere auch § 6 HalblSchG, der einen besonderen Schutz für Topographien vorsieht, aber zugleich in Abs. 2 bestimmte Handlungen nicht dem Schutz unterstellt.
35 Wohingegen hier die Einschränkungen des § 69e UrhG (Dekompilierung) zu beachten wären.
36 S. auch *Brammsen*, in: Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl. 2014, § 17, Rn. 55.
37 *Brammsen*, in Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl. 2014, § 17, Rn. 57, 60 f.
38 *Brammsen*, in Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl. 2014, § 17, Rn. 57 m. w. N.
39 Ausführlich hierzu *von Pelchrzim*, CCZ 2009, 25 ff.; *Brammsen*, in: Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl. 2014, § 17, Rn. 57, 60 f.

Die Know-how-Schutz-Richtlinie hingegen sieht nunmehr in Art. 5 ausdrücklich Ausnahmen vom Grundsatz der Rechtswidrigkeit des Geheimnisverrats vor. Insbesondere zur Aufdeckung eines beruflichen oder sonstigen Fehlverhaltens oder einer illegalen Tätigkeit soll Geheimnisverrat erlaubt sein, sofern der Whistleblower in der Absicht handelte, das allgemeine öffentliche Interesse zu schützen. Insofern knüpft jedenfalls die Richtlinie nicht an die Angemessenheit der Reaktion an, sodass abzuwarten sein wird, ob die deutsche Umsetzung ein solches Merkmal – jedenfalls für externes Whistleblowing – vorsehen wird.

2. Exkurs: Kartellrechtliche Behandlung von Whistleblowern

Seit 2000 betreibt das Bundeskartellamt ein eigenes „Kronzeugenprogramm", Bonusregelung genannt, welches zuletzt im Jahr 2006 grundlegend überarbeitet wurde.[40] Jeder Kartellbeteiligte kann dabei von dieser Bonusregelung Gebrauch machen und als Whistleblower auftreten. Dem Kartellbeteiligten, der sich als erster an das Bundeskartellamt wendet (sogenannter Whistleblower), wird das drohende Bußgeld vollends erlassen. Gleiches gilt, wenn dem Bundeskartellamt nach Eröffnung des Verfahrens entscheidende Beweise vorgelegt werden. Für alle übrigen Beteiligten kann sich das Bußgeld um bis zu 50 % reduzieren, je nachdem wie viel sie zum Nachweis eines Kartells beigetragen haben.

Das Bundeskartellamt und andere Behörden versuchen durch solche Kronzeugen- und Bonusregelungen den Beweisschwierigkeiten, mit denen sie im Laufe der Ermittlungen konfrontiert werden, zu begegnen und sich Insiderinformationen zu beschaffen und diese zu verwenden. Mit zunehmendem Erfolg, wie die Entscheidung in Sachen Bierkartell, Anheuser Busch kein Bußgeld aufzuerlegen,[41] imposant darlegt.

Nach Angaben des Bundeskartellamts wird mittlerweile jedes zweite Kartellverfahren des Bundeskartellamts durch Hinweise von Kronzeugen ausgelöst.[42] Die Bonusregelung führt nicht nur dazu, dass Kartelle aufgedeckt werden, von denen das Bundeskartellamt nur schwer oder überhaupt keine Kenntnis erlangt hätte, sondern auch dazu, dass innerhalb des Kartells eine erhebliche Unsicherheit besteht: So ist unklar, ob und gegebenenfalls wer als erster das Schweigen bricht und das Kartell beim Bundeskartellamt zur Anzeige bringt.

Eine Übertragung dieser Straffreiheit für die „Selbstanzeige" dürfte vorliegend angesichts des Analogieverbots im Strafrecht nicht in Betracht kommen, obgleich die „Selbstanzeige" in Form der tätigen Reue dem Strafrecht nicht unbekannt ist.[43]

VII. Prozessuales

Geheimnisschutz spielt auch in prozessualer Hinsicht eine wichtige Rolle. So stellen sich nicht nur Fragen, welche Ansprüche mit einem Geheimnisverrat einhergehen, sondern auch wie diese Ansprüche durchgesetzt werden können und was mit den Geheimnissen während des Prozesses selbst geschieht.

1. Durchsetzung des Geheimnisschutz

Betroffenen Unternehmen gibt die Richtlinie nunmehr auch einen umfangreicheren Maßnahmenkatalog zur gerichtlichen Durchsetzung des Geheimnisschutzes an die Hand und nähert den Know-how-Schutz damit stark dem Schutz von gewerblichen Schutzrechten an. Unterschieden wird insbesondere zwischen vorbeugenden und repressiven Maßnahmen.

a) Vorläufige und vorbeugende Maßnahmen

Art. 10 der Richtlinie sieht vor, dass die zuständigen Gerichte auf Antrag des Inhabers des Geschäftsgeheimnisses bestimmte vorläufige oder vorbeugende Maßnahmen gegen den angeblichen Rechtsverletzer beantragen können. Hierzu gehören insbesondere die vorläufige Einstellung der Nutzung oder Offenlegung der Geheimnisse, ein Verbot der Nutzung, Herstellung, Anbietens oder Vermarktens rechtsverletzender Produkte sowie deren Beschlagnahme oder Herausgabe.

Diese Maßnahmen sind an die Bedingung geknüpft, dass der Antragsteller (also der Inhaber des Geschäftsgeheimnisses) alle vernünftigerweise verfügbaren Beweise vorlegt, damit sich die Gerichte mit ausreichender Sicherheit davon überzeugen können, dass ein Geschäftsgeheimnis vorliegt, dessen Inhaber der Antragsteller ist und welches der Antragsgegner rechtswidrig erlangt oder genutzt hat, Art. 11 Abs. 1 der Richtlinie. So soll sichergestellt werden, dass etwaige vorläufige Entscheidungen des Gerichts auf eine profunde Tatsachenbasis gestellt und nicht lediglich Konkurrenten in der Ausübung ihrer Geschäfte behindert werden.

Das Gericht hat bei seiner Entscheidung und der Beurteilung der Verhältnismäßigkeit stets die Belange des konkreten Einzelfalls zu berücksichtigen. Art. 11 Abs. 2 der Richtlinie sieht ferner einen umfassenden Katalog an Kriterien vor, die das Gericht gegebenenfalls zu berücksichtigen hat. Hierzu gehören neben dem Wert des Geschäftsgeheimnisses unter anderem auch die zum Schutz des Geschäftsgeheimnisses getroffenen Maßnahmen, die Folgen der rechtswidrigen Nutzung oder Offenlegung sowie Interessen Dritter und der Öffentlichkeit. Insofern zieht sich auch hier der rote Faden konsequent durch: Sofern keine Vorkehrungen zum Geheimnisschutz getroffen werden, wird ein solcher nicht gewährt.

Neben den vorläufigen und vorbeugenden Maßnahmen kann das Gericht nach Art. 10 Abs. 2 der Richtlinie jedoch auch anordnen, dass die Fortsetzung der Nutzung eines Geschäftsgeheimnisses an die Stellung einer oder mehrerer Sicherheiten geknüpft ist, die eine Entschädigung des Inhabers sicherstellen. Die Offenlegung eines Geschäftsgeheimnisses darf hingegen nicht erlaubt werden.

b) Maßnahmen aufgrund einer Sachentscheidung

Die Richtlinie sieht, ähnlich wie auch schon die Enforcement-Richtlinie[44] zur Durchsetzung gewerblicher Schutzrechte, eine Reihe von gerichtlichen Maßnahmen vor, die zum Schutz vor Geheimnisverrats erlassen werden können. Neben den obligatorischen Unterlassungsanordnungen hinsichtlich des Verrats sowie der Nutzung von Geschäftsgeheimnissen oder dem Vertrieb oder der Herstellung rechtsverletzender Produkte kann das Gericht auch die Vernichtung bzw. den Rückruf der Gesamtheit oder eines Teils der Dokumente, Gegenstände, Materialien, Stoffe oder elektronischen Dateien, die das Geschäftsgeheimnis enthalten oder verkörpern anordnen, Art. 12 Abs. 1

40 Bundeskartellamt, Bekanntmachung Nr. 9/2006 über den Erlass und die Reduktion von Geldbußen in Kartellsachen – Bonusregelung – vom 7.3.2006; vgl. zur Bonusregelung auch *Mundt*, CB 2013, 81, 83.
41 Bundeskartellamt, Fallbericht vom 9.5.2016, Az.: B10-20/15 – Bierkartell.
42 Bundeskartellamt – Bonusregelung, abrufbar unter www.bundeskartellamt.de/DE/Kartellverbot/Bonusregelung/bonusregelung_node.html (Abruf: 29.9.2016).
43 S. §§ 261 Abs. 9, 266a Abs. 6 StGB.
44 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums.

der Richtlinie. Auch die Herausgabe dieser Daten an den Antragsteller kann angeordnet werden, Art. 12 Abs. 1d der Richtlinie.
Die Kosten für diese Maßnahmen hat regelmäßig der Rechtsverletzer zu tragen, Art. 12 Abs. 4 der Richtlinie. Auch bei der Anordnung von Maßnahmen aufgrund einer Sachentscheidung hat das Gericht die konkreten Umstände des Einzelfalls zu berücksichtigen, Art 13.[45]
Sofern der Rechtsverletzer wusste oder hätte wissen müssen, dass er einen rechtswidrigen Erwerb oder eine rechtswidrige Nutzung oder Offenlegung eines Geschäftsgeheimnisses vornahm, haben die Gerichte die Möglichkeit, dem Antragsteller einen Schadensersatzanspruch zuzusprechen. Dieser umfasst den Schaden, der dem Schaden, den der Inhaber des Geschäftsgeheimnisses infolge des rechtswidrigen Erwerbs bzw. der Offenlegung oder Nutzung tatsächlich erlitten hat, angemessen ist, Art. 14 Abs. 1. Die Höhe bemisst sich – auch hier – nach den Umständen des Einzelfalls. Alternativ hierzu kann die im gewerblichen Rechtsschutz bereits etablierte Lizenzanalogie herangezogen werden, nach der die fiktive Lizenzgebühr als Schaden herangezogen werden kann, Art. 14 Abs. 2.
Der Vollständigkeit halber sei noch erwähnt, dass das Gericht die Verbreitung von Informationen über die betreffende Entscheidung anordnen kann, einschließlich der vollständigen oder teilweisen Veröffentlichung der Gerichtsentscheidung, Art. 15.

2. Geheimnisschutz während des Verfahrens

Geheimnisse sind keine Geheimnisse, wenn sie in aller Öffentlichkeit diskutiert werden. Gerichtsverfahren hingegen sind in der Regel öffentlich, sodass hier eine Diskrepanz zwischen Geheimnisschutz und Öffentlichkeit besteht. Zur Verbesserung und Wahrung des Geheimnisschutzes sieht Art. 9 der Richtlinie strenge Regeln vor, unter denen über Geheimnisverrat verhandelt werden soll. Nach Art. 9 Abs. 1 sind daher die Parteien und ihre Rechtsanwälte sowie Gerichtsbedienstete, Zeugen, Sachverständigen und alle sonstigen am Verfahren beteiligten Personen nicht befugt, ein (angebliches) Geschäftsgeheimnis zu nutzen oder offenzulegen. Das Gericht kann auch vorsehen, dass der Zugang zu in den Prozess eingebrachten Dokumenten oder Geheimnisträgern nur einer begrenzten Anzahl von Personen ermöglicht wird, Art. 9 Abs. 2.[46]
Dies soll es Inhabern von Geheimnissen erleichtern, die Gerichte anzurufen. Denn häufig stellt es für diese bereits eine hohe Hürde dar, die verletzten Geheimnisse im Prozess zu offenbaren. Ohne eine (jedenfalls begrenzte) Offenlegung des Geheimnisses bestehen keine Erfolgsaussichten der Klage,[47] und dies auf zwei Ebenen: zum einen bereits bei der Informationsbeschaffung und zum anderen falls Know-how Streitgegenstand sein sollte. Dieses Problem mit rechtsstaatlichen Mitteln zu lösen, die sich in das bestehende System der deutschen Gerichtsbarkeit einfügen, ist nunmehr (keine leichte) Aufgabe des deutschen Gesetzgebers. Vorschläge, wie das *Düsseldorfer Verfahren,*[48] *Black-Box-Verfahren*[49] oder das *In-Camera-Verfahren*[50] gab es bereits in der Vergangenheit – jedoch waren auch sie nicht kritiklos und sind auf ein Know-how-Verfahren nur bedingt anwendbar.[51]

VIII. Geheimnisschutz in der Praxis

Obgleich die Richtlinie noch nicht in deutsches Recht umgesetzt wurde, dürfte sich für Unternehmen empfehlen, bereits jetzt Vorbereitungen zum Schutz des vorhandenen Know-hows zu treffen. Denn, wie bereits mehrfach erwähnt, wird Know-how-Schutz nach der Richtlinie nur dann gewährt, wenn entsprechende Schutzmaßnahmen getroffen wurden – ohne Vorsorge, kein Schutz. Und dabei dürfte gelten, dass die Qualität der Schutzmaßnahmen mit der Bedeutung des Know-hows steigen sollte.
Sein Know-how angemessen zu schützen, ist eine fordernde Aufgabe für Unternehmen. Neben der Frage, was als Know-how zu schützen ist, stellen sich zahlreiche Fragen, wie das vorhandene Know-how zu schützen ist. Insofern empfiehlt sich ein schrittweises Vorgehen:
Zunächst sollte bestehendes und potenzielles Know-how identifiziert werden. Dies können bestehende Gewerbliche Schutzrechte wie Patente sein, aber auch Urheberrechte oder nicht schutzfähiges Wissen, wie beispielsweise die geheime Zutat einer erfolgreichen Limonade. Hierbei wird nicht nur aufgedeckt, welche Geheimnisse schützenswert sind, sondern auch, wo bereits Schutzlücken innerhalb des Unternehmens bestehen. Zeitgleich zur Identifikation des Know-hows sollte auch die Identifikation der Know-how-Träger erfolgen. Hier empfiehlt sich insbesondere auch die Einschaltung der Personalabteilung sowie die Prüfung der jeweiligen Arbeitsverträge auf etwaig bestehende Wettbewerbsverbote oder Geheimhaltungsklauseln.
Im Anschluss an die Identifikation des Status quo empfiehlt sich, ein maßgeschneidertes Schutzkonzept zu entwickeln, dass den Bedürfnissen des Unternehmens gerecht wird und alle Besonderheiten ausreichend berücksichtigt. Wie später noch aufgezeigt werden wird, gibt es zahlreiche Möglichkeiten, wie Know-how abfließen kann und welche Schutzmaßnahmen man hiergegen ergreifen kann. Berücksichtigt werden sollten hierbei auch die tatsächlichen Möglichkeiten: Beschränken begrenzte Finanzmittel die möglichen Maßnahmen? Genügen juristische Vorkehrungen oder sollte auch ein technischer Schutz installiert werden? Besteht eine hohe Fluktuation auf Arbeitnehmerseite? Wird viel gereist? Gibt es Kooperationen mit anderen Unternehmen?
Je nachdem wie die Evaluation des Unternehmens ausfällt, bestehen zahlreiche unterschiedliche Möglichkeiten, das bestehende Know-how zu schützen. Neben technischen Vorkehrungen (Installation einer Firewall; Beschränkung des USB-Zugriffs) sind es insbesondere juristische Mittel, die dies bewerkstelligen können. Aus arbeitsrechtlicher Sicht sollten die bestehenden und künftigen Arbeitsverträge überarbeitet werden (insbesondere sollten Wettbewerbsverbote aufgenommen und vom Arbeitnehmer etwaige Nutzungs- und Verwertungsrechte eingeräumt werden) und insbesondere mit Geheimnisträgern ein gesondertes Non-Disclosure Agreement (NDA – Geheimhaltungsvereinbarung) abgeschlossen werden. Je nach Situation des Un-

45 Hierzu s. bereits oben unter VII.1. a).
46 Zu der hierdurch aufkommenden Frage der Abwägung des Öffentlichkeitsgrundsatzes auf der einen und der Wahrung des Geheimhaltungsinteresses auf der anderen Seite siehe auch *McGuire*, GRUR 2015, 424, 427 ff.
47 Siehe auch *McGuire*, GRUR 2015, 424, 427 f. m. w. N.; *Stadler*, NJW 1989, 1202.
48 Hierbei handelt es sich um eine Art selbständiges Beweisverfahren, das sich dem Problem widmet, dass die Auskunftspflicht gerade der Feststellung der Verletzung dient, der angebliche Verletzte hierzu aber sensible Informationen offenlegen muss.; s. hierzu insbesondere *McGuire*, GRUR 2015, 424, 430 m. w. N.
49 Das Black-Box-Verfahren – oder auch bekannt als Wirtschaftsprüfervorbehalt – sieht vor, dass sich ein zur Verschwiegenheit verpflichteter Dritter mit der Beantwortung der streitgegenständlichen Frage befasst und ausschließlich ihm – und nicht etwa auch dem Gericht – die sensiblen Informationen zur Verfügung gestellt werden; das Gericht selbst stützt seine Entscheidung dann auf den Feststellung des Dritten; siehe auch *McGuire*, GRUR 2015, 424, 430 f., welche einen Verstoß gegen den Unmittelbarkeitsgrundsatz als gegeben sieht.
50 Hierbei wird die zu schützende Information dem Gericht offenbart, dem Gegner jedoch vorenthalten; s. insbesondere *McGuire*, GRUR 2015, 424, 430 ff. sowie 433 f. m. w. N., welche sich auch mit entsprechender Rechtsprechung detailliert auseinandersetzt und die grundsätzliche Zulässigkeit der Beschränkung des rechtlichen Gehörs einer der Parteien diskutiert.
51 Statt vieler *McGuire*, GRUR 2015, 424, 430 ff. m. w. N. sowie eigenen umfangreichen Regelungsvorschlägen; *Hauck*, NJW 2016, 2218, 2222.

ternehmens empfiehlt es sich, mehrere unterschiedliche Varianten vorzuhalten. Darüber hinaus kann es sich empfehlen, einzelnen Mitarbeitern nur so viel Zugriff auf unternehmensinternes Know-how zu gewähren, wie für die jeweilige Arbeit erforderlich ist (*need to know*). Auch die Installation einer Travel Policy kann sich empfehlen, wenn die Mitarbeiter häufig in Länder reisen, in denen der Zoll auch eine Untersuchung der Inhalte auf Telefon und Computer vornehmen kann (beispielsweise in den USA).

In den gesamten Prozess eingezogen werden sollten nicht nur interne und/oder externe Juristen, sondern auch die Unternehmensführung sowie das Personalwesen. Von besonderer Bedeutung wird auch die Einbindung der IT-Abteilung sein, um das entwickelte Schutzkonzept auch auf technischer Ebene umzusetzen.

Ist der Know-how-Schutz installiert und ein Abfluss von Know-how erschwert oder gar verhindert, empfiehlt sich dennoch eine aktive Beobachtung des internen Know-hows sowie der Wettbewerber, um den Abfluss von Know-how schnellstmöglich zu erkennen und die entsprechenden repressiven Maßnahmen in die Wege zu leiten. Denn die Richtlinie gewährt nicht nur strafrechtlichen Schutz, dem Verletzten stehen vielmehr auch Auskunfts-, Rückrufs-, Vernichtungs-, Unterlassungs- und Schadensersatzansprüche gegen den Verletzer zu.

IX. Fazit

Aus deutscher Sicht bleibt das grundlegende Schutzkonzept unverändert. Der Rechtsschutz von Geschäftsgeheimnissen bietet keinen exklusiven Schutz immaterieller Vermögensgüter selbst.[52] Auch nach Umsetzung der Richtlinie wird der Geheimnisschutz in erster Linie ein Zugangsschutz sein.[53] Neue Ausschließlichkeitsrechte für Geschäftsgeheimnisse sieht die Richtlinie nicht vor, auch wenn der Geheimnisschutz in seinen Rechtsfolgen einem absoluten Recht angenähert wird. Geschützt wird lediglich die Geheimnissphäre, nicht jedoch die Informationen selbst. Anders als bislang im deutschen Recht wird der Geheimhaltungswille nicht vermutet werden. Geheimnisschutz kann nur dann erfolgreich geltend gemacht werden, wenn bewiesen werden kann, dass die betreffenden Informationen Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen waren. Dazu bedarf es eines strategischen Know-how-Schutzkonzeptes sowie ein Informationsmanagement. Somit gehört Know-how-Schutz zur unternehmerischen Compliance.

Anne Baranowski, LL.M., ist Rechtsanwältin bei Schalast Rechtsanwälte & Notare in Frankfurt a. M. und berät vor allem im Urheber-, IP/IT- und Wettbewerbsrecht, zum Datenschutz sowie zu Compliance-Themen.

Ramón Glaßl, LL.M., ist Rechtsanwalt bei Schalast Rechtsanwälte & Notare in Frankfurt a. M. und berät Mandanten insbesondere aus der TMT-Branche in Fragen unter anderem des gewerblichen Rechtsschutzes und des Kartellrechts.

52 *Dorner*, FAZ, vom 18.2.2015, 18.
53 *Hauck*, NJW, 2016, 2218, 2221.

BGH: Für das Stiftungskollisionsrecht gelten die Grundsätze des Internationalen Gesellschaftsrechts

BGH, Urteil vom 8.9.2016 – III ZR 7/15
ECLI:DE:BGH:2016:080916UIIIZR7.15.0
Volltext des Urteils: **BB-ONLINE BBL2016-2369-3**
unter www.betriebs-berater.de

LEITSÄTZE

a) Für das Stiftungskollisionsrecht ist auf die Grundsätze des Internationalen Gesellschaftsrechts zurückzugreifen.

b) Das Personalstatut der Stiftung ist auch für die Rechtsstellung als Destinatär und die daraus folgenden Ansprüche maßgeblich.

ZPO § 293, § 563 Abs. 4

SACHVERHALT

Die Klägerin ist eine in Österreich eingetragene und dort ansässige Privatstiftung, deren Zweck neben der Sicherung des Stiftungsvermögens und der Erhaltung und Pflege historischer Bauten die Unterstützung der jeweiligen Begünstigten aus den Erträgen des Stiftungsvermögens ist. Sie begehrt mit ihrer Klage die Feststellung, dass die Beklagte nicht mehr Begünstigte sei und sie keine Ansprüche auf Zahlung von Bezügen habe.

Die Stifterin errichtete am 21. April 2005 vor einem Notar in E. (Österreich) eine Stiftungszusatzurkunde, in welcher die Beklagte als Begünstigte benannt wird.

Bis einschließlich April 2009 erhielt die Beklagte monatliche Zuwendungen von der Klägerin. Danach erfolgten im März und im Mai 2010 nochmals zwei Einmalzahlungen.

Die Klägerin ist der Ansicht, die ursprüngliche Begünstigtenstellung der Beklagten sei entfallen. Dies ergebe sich daraus, dass sie in zwei weiteren Stiftungszusatzurkunden vom 8. November 2007 und vom 12. Juni 2012 – was insoweit unstreitig ist – nicht mehr als Begünstigte aufgeführt werde.

Das LG hat die Klage abgewiesen. Auf die Berufung der Klägerin hat das OLG das erstinstanzliche Urteil abgeändert und festgestellt, dass