

# Stellungnahme

## Regierungsentwurf zur Umsetzung der Know-how-Richtlinie

14. Oktober 2018

Seite 1

### Zusammenfassung

Am 18. Juli 2018 hat die Bundesregierung den Regierungsentwurf des Gesetzes zum Schutz von Geschäftsgeheimnissen (folgend „GeschGehG-E“) beschlossen. Bitkom begrüßt es, dass mit dem GeschGehG-E ein eigenes nationales Stammgesetz zum Schutz von Geschäftsgeheimnissen geschaffen und damit ihrer wirtschaftlichen Bedeutung Rechnung getragen wird.

Die inhaltliche Entwicklung der Richtlinienumsetzung ist insgesamt positiv zu bewerten. Zahlreiche Änderungsanregungen aus unserer Stellungnahme vom 18. Mai 2018 zum Referentenentwurf (folgend „Ref-E“) des GeschGehG-E haben Eingang in den Regierungsentwurf (folgend „Reg-E“) gefunden. Auch hat der Entwurf teils strukturelle Verbesserungen (§§ 1, 2 Reg-E) und sinnvollere Formulierungen erfahren.

Zum Reg-E nehmen wir im Folgenden Stellung und ergänzen unsere zum Ref-E geäußerten Anmerkungen, soweit erforderlich. Positiv hervorzuheben ist zunächst, dass der Begriff des Geschäftsgeheimnisses entsprechend der Richtlinie legal definiert wird. Die Definition sollte beibehalten werden. Bitkom begrüßt es, dass das Erfordernis der „angemessenen Geheimhaltungsmaßnahmen“ nicht weiter konkretisiert wird. Die allgemein gehaltene Formulierung ermöglicht es, flexibel eine Vielzahl von Einzelfällen unter das Gesetz subsumieren und auf etablierte Prinzipien technischer und organisatorischer Maßnahmen im Unternehmen zurückgreifen zu können.

- Die Definition des rechtsverletzenden Produkts hingegen überzeugt, wie bereits im Ref-E, nicht vollends. Hier ist anzumerken, dass im Fall von Marketing mit dem rechtsverletzenden Produkt nicht das beworbene Produkt gemeint sein darf. Betrachtet man die Definition im Zusammenhang mit den Ansprüchen bei Rechtsverletzungen, muss klargestellt werden, dass in diesen Fällen Ansprüche auf Rückruf und Vernichtung des beworbenen Produkts ausgeschlossen sind. Vielmehr kann in diesen Fällen nur eine Dienstleistung, nämlich die Marketingtätigkeit, das rechtsverletzende Produkt sein. Marketing und Produkt sind getrennt zu beurteilen, um unbillige Ergebnisse zu vermeiden.
- Positiv zu bewerten ist wiederum die nunmehr nahe Orientierung an der Richtlinienvorgabe bzgl. der Inhaberschaft eines Geschäftsgeheimnisses. Während der Ref-

Bundesverband  
Informationswirtschaft,  
Telekommunikation  
und Neue Medien e.V.

**Judith Steinbrecher, LL.M.**  
**Bereichsleiterin Gewerblicher  
Rechtsschutz & Urheberrecht**

T +49 30 27576-155  
j.steinbrecher@bitkom.org

Albrechtstraße 10  
10117 Berlin

Präsident  
Achim Berg

Hauptgeschäftsführer  
Dr. Bernhard Rohleder

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 2|16

E noch auf die rechtmäßige Erlangung und Erlaubnis zur Nutzung und Offenlegung abstellte, beschränkt sich der Reg-E auf die Voraussetzung der rechtmäßigen Kontrolle über ein Geschäftsgeheimnis. Dies ist vorteilhaft mit Blick auf Lizenznehmer, denn diese sollten nicht zwangsläufig in den Kreis der Geschäftsgeheimnisinhaber aufgenommen werden. Vielmehr sollten hier die jeweiligen Lizenzverträge maßgebend sein.

- Erfreulich ist, dass das sog. „Reverse Engineering“ grundsätzlich zulässig sein soll, da durch das Analysieren konkurrierender Produkte Innovationen gefördert werden können. Ein vertraglicher Ausschluss muss entsprechend der Richtlinienvorgabe in Art. 3 Abs. 1 b) a.E. jedoch weiterhin möglich sein.
- Auch die Privilegierung von Whistleblowing begrüßen wir. Das GeschGehG muss jedoch eine abgestufte Herangehensweise vorsehen, mit dem Unternehmen die Möglichkeit gegeben wird, ein intern verpflichtendes Schutzkonzept zu implementieren und damit frühzeitig einer nicht gerechtfertigten Rufschädigung des Unternehmens begegnen zu können.
- Erfreulich ist die im Reg-E erfolgte Anpassung des Umfangs von Ordnungsgeld und Ordnungshaft. Die inzwischen vorgesehenen Grenzen werden den Anforderungen der Richtlinie nach wirksamen, verhältnismäßigen und abschreckenden Sanktionen deutlich besser gerecht, als der im Ref-E vorgesehene, äußerst niedrige Rahmen.

### Im Einzelnen

Am 5. Juli 2016 trat die Richtlinie des Europäischen Parlamentes und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung in Kraft. Ziel der Richtlinie ist es, einen europaweit einheitlichen Mindeststandard zu schaffen, um Geschäftsgeheimnisse vor dem rechtswidrigen Erwerb, der rechtswidrigen Nutzung sowie der rechtswidrigen Offenlegung zu schützen.

Das GeschGehG soll diese Richtlinie umsetzen. Seit dem 18. Juli 2018 wird nun der Reg-E zum GeschGehG beraten.

Wir begrüßen die Entscheidung, den Schutz von Geschäftsgeheimnissen, der bislang lediglich als Querschnittsmaterie in unterschiedlichen Gesetzen geregelt wurde, nunmehr

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 3|16

in einem Gesetz zu bündeln. Auch in ausländischen Rechtsordnungen wird der Weg, ein eigenes Gesetz für den Geheimnisschutz vorzuhalten, gewählt.<sup>1</sup>

In der politischen Debatte müssen aber auch sich abzeichnende europäische Entwicklungen wie die zum Schutz von Whistleblowern berücksichtigt werden. Der Entwurf enthält nach der zwischenzeitlich geänderten Paragraphenreihenfolge nunmehr in § 5 Nr. 2 Reg-E GeschGehG-E<sup>2</sup> eine Privilegierung von Whistleblowern. Danach ist die Erlangung, Nutzung oder Offenlegung eines Geschäftsgeheimnisses gerechtfertigt, wenn dies zum Schutz eines berechtigten Interesses erfolgt, insbesondere zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die das Geschäftsgeheimnis erlangende, nutzende oder offenlegende Person in der Absicht handelt, das allgemeine öffentliche Interesse zu schützen (weitere Ausführungen zu § 5 Nr. 2 siehe unten unter 6.2). Die Kommission hat zwischenzeitlich (23. April 2018) aber auch einen Entwurf einer sog. Whistleblower-Richtlinie veröffentlicht, die zum Ziel hat, Whistleblower weiter zu schützen. Der GeschGehG-E regelt damit nun vorab einen Bereich, der von der geplanten Whistleblower-Richtlinie neu beeinflusst werden wird. Es sollte daher nicht etwas in Umsetzung einer bestehenden Richtlinie geregelt werden, obwohl bereits absehbar ist, dass eine weitergehende Regelung erforderlich sein wird. Tritt der Gesetzesentwurf so in Kraft, müssen Unternehmen ihre Prozesse zum Geheimnisschutz an die neue Rechtslage anpassen. Wird die Regelung kurze Zeit später durch die Umsetzung der kommenden Whistleblower-Richtlinie verändert, sind die Unternehmen gehalten, ihre Prozesse erneut zu verändern. Dies führt zu einer unwirtschaftlichen Belastung und im Endeffekt auch dazu, dass die Änderungen nicht mit voller Kraft vorgenommen werden. Daher sollten diese Entwicklungen bereits jetzt berücksichtigt werden.

### 1. Definition „Geschäftsgeheimnis“, § 2 Nr. 1

Die Definition des Begriffs „Geschäftsgeheimnis“ ist im Hinblick auf die Umsetzung der Richtlinie von entscheidender Bedeutung; so heißt es in **Erwägungsgrund 14** der Richtlinie:

*„Es ist wichtig, eine **homogene Definition** des Begriffs „Geschäftsgeheimnis“ festzulegen, ohne den vor widerrechtlicher Aneignung zu schützenden Bereich einzuzengen. Eine solche Definition sollte daher so beschaffen sein, dass sie Know-how, Geschäftsinformationen und technologische Informationen abdeckt, bei denen so*

<sup>1</sup> So z.B. in den USA (“Uniform Trade Secrets Act” von 1979 und 1985, “Defend Trade Secrets Act of 2016”).

<sup>2</sup> Die folgenden Paragraphen sind, sofern nicht anders gekennzeichnet, solche des Reg-E GeschGehG.

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 4|16

*wohl ein legitimes Interesse an ihrer Geheimhaltung besteht als auch die legitime Erwartung, dass diese Vertraulichkeit gewahrt wird. Darüber hinaus sollten solches Know-how oder solche Informationen einen — realen oder potenziellen — Handelswert verkörpern. Solches Know-how oder solche Informationen sollten so verstanden werden, dass sie einen Handelswert verkörpern, zum Beispiel wenn ihr unbefugter Erwerb oder ihre unbefugte Nutzung oder Offenlegung die Interessen der Person, die rechtmäßig die Kontrolle über sie ausübt, aller Voraussicht nach dadurch schädigt, dass das wissenschaftliche oder technische Potenzial, die geschäftlichen oder finanziellen Interessen, die strategische Position oder die Wettbewerbsfähigkeit dieser Person untergraben werden. Die Definition eines Geschäftsgeheimnisses schließt belanglose Informationen und die Erfahrungen und Qualifikationen, die Beschäftigte im Zuge der Ausübung ihrer üblichen Tätigkeiten erwerben, sowie Informationen aus, die den Personenkreisen, die üblicherweise mit derartigen Informationen umgehen, generell bekannt sind bzw. für sie leicht zugänglich sind.“*

Ein „Geschäftsgeheimnis“ wird nun in § 2 Nr. 1 legaldefiniert als

*„eine Information, die*

*a) 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) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist.“*

Die gewählte und gegenüber dem Ref-E nur noch leicht veränderte Definition orientiert sich sehr nahe am Wortlaut der Richtlinienvorgabe.

Das deutsche Recht kennt den Begriff des Geschäftsgeheimnisses auch in anderen Gesetzen, differenziert dabei jedoch noch zwischen Betriebs- und Geschäftsgeheimnis. Der Begriff des Betriebsgeheimnisses zielt auf Kenntnisse und Tatsachen im Bereich der Technik ab, während Geschäftsgeheimnisse primär im kaufmännischen Bereich angesiedelt sind. Nach der ständigen Rechtsprechung wird dabei unter einem Geschäfts- und Betriebsgeheimnis jede im Zusammenhang mit einem Betrieb stehende Tatsache verstanden, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 5|16

und nach dem Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheim gehalten werden soll.<sup>3</sup> Nach § 17 UWG gehört zu den wesentlichen Merkmalen des Geschäfts- und Betriebsgeheimnisses, dass der Betriebsinhaber einen begründeten Geheimhaltungswillen hat. Dieser Wille soll ein Geheimnis von dem bloßen Unbekannt sein einer Tatsache unterscheiden.<sup>4</sup> Dieser Wille zeigt sich zwar bislang schon häufig in entsprechenden Geheimhaltungsvereinbarungen, kann sich jedoch auch lediglich aus den Umständen ergeben. Nach der Rechtsprechung des BGH dürfen an die Manifestation des Geheimhaltungswillens keine überzogenen Anforderungen gestellt werden. So soll es im Einzelfall genügen, wenn sich dieser Wille aus der Natur der geheim zu haltenden Tatsache ergibt.<sup>5</sup> In einer anderen Entscheidung hat der BGH den Geheimhaltungswillen damit begründet, dass bei komplexeren Gegenständen der Wille zur Geheimhaltung aufgrund der wirtschaftlichen Bedeutung „ohne Weiteres“ anzunehmen sei.<sup>6</sup> Im innerbetrieblichen Streitfall liegt die Beweislast eher beim Arbeitnehmer.<sup>7</sup>

Der praxisrelevante Unterschied zwischen dem GeschGehG-E und dem bisherigen deutschen Recht im Hinblick auf den Begriff „Geschäftsgeheimnis“ besteht somit darin, dass es die in § 2 Nr. 1 b) vorausgesetzten „angemessenen Geheimhaltungsmaßnahmen“ bisher in Deutschland nicht gab und der deutsche Begriff insofern weiter gefasst war. Der Geheimnisinhaber musste bislang nicht nachweisen, dass er Maßnahmen zum Schutz vertraulicher Informationen tatsächlich getroffen hat.

Wir begrüßen es, dass die angemessenen Geheimhaltungsmaßnahmen nicht selbst legal definiert wurden. Zwar ist der Begriff „angemessene Geheimhaltungsmaßnahmen“ sehr allgemein gehalten und führt zunächst zu einer gewissen Rechtsunsicherheit. Eine weitere Konkretisierung im Gesetz würde aber zu weniger Flexibilität führen und würde risikieren, bestimmte, eigentlich geeignete Maßnahmen ungewollt auszuklammern. Wie in der Gesetzesbegründung richtig ausgeführt, kann es sich bei Geheimhaltungsmaßnahmen sowohl um physische Zugangsbeschränkungen und Vorkehrungen handeln, als auch um vertragliche Sicherungsmechanismen. Auch sonstige technische – etwa virtuelle –, oder rechtliche Schutzvorkehrungen in den Organisationsprozessen kämen in Frage. Eine Heranziehung der Gesetzesbegründungsmaterialien bei der Auslegung des Begriffs der Angemessenheit bietet damit die nötige Rechtssicherheit.

Unserer in der Stellungnahme zum Ref-E geäußerten Anmerkung folgend, dem Begriff der angemessenen Geheimhaltungsmaßnahmen sei das Kriterium der Verhältnismäßigkeit hinzuzufügen, wurde im Reg-E begrüßenswerter Weise die Formulierung „den Umständen

<sup>3</sup> *Harte-Bavendamm/Henning-Bodewig/Harte-Bavendamm*, UWG, § 17, Rn. 1-1b, m.w.N.

<sup>4</sup> BGH, GRUR 1964, 31.

<sup>5</sup> BGH, NJW 1995, 2301.

<sup>6</sup> BGH, GRUR, 1977, 539, 540.

<sup>7</sup> Vgl. *Harte-Bavendamm/Henning-Bodewig/Harte-Bavendamm*, UWG, § 17, Rn. 5.

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 6|16

nach“ ergänzt. Dadurch rückt der Gesetzesentwurf mit seinem Wortlaut näher an die Richtlinienvorgabe und trägt dem Erfordernis der Verhältnismäßigkeit besser Rechnung.

Wir sind der Ansicht, dieses Kriterium sollte zumindest beibehalten, oder ausdrücklich durch das Wort „Verhältnismäßig“ ersetzt werden.

Eine Geheimhaltungsmaßnahme kann nur dann angemessen sein, wenn der Aufwand nicht völlig außer Verhältnis zum anzunehmenden Nachteil bei Verlust dieser Geheimniserhaltung steht.

Vermieden werden sollte in jedem Fall, durch eine zu enge Fassung des Anwendungsbereichs des Gesetzes das Schutzniveau zu reduzieren.

### 2. Definition „rechtsverletzendes Produkt“, § 2 Nr. 4

In § 2 Nr. 4 wird ein rechtsverletzendes Produkt als ein Produkt, dessen Konzeption, Merkmale, Funktionsweise, Herstellungsprozess oder Marketing in erheblichem Umfang auf einem rechtswidrig erlangten, genutzten oder offengelegten Geschäftsgeheimnis beruht, definiert. Die so formulierte Begriffsbestimmung entspricht wortwörtlich der Definition in der Richtlinie, wo sie trotz anhaltender Kritik<sup>8</sup> beibehalten wurde. Nach dieser Definition lässt auch das Marketing eines Produkts mit Hilfe von rechtswidrig erlangten, genutzten oder offengelegten Geheimnissen das so beworbene Produkt zu einem „rechtsverletzenden Produkt“ werden.

In Verbindung mit den Ansprüchen aus § 7 (z.B. Rückruf und Entfernung vom Markt) geht diese Definition deutlich über das gerechtfertigte Schutzinteresse hinaus.

Beispiel: A und B sind Konkurrenten, beide beliefern den Kunden K mit dem substituierbaren Produkt P. Durch einen Geheimnisverrat eines ehemaligen Angestellten von A erlangt B Informationen über As Finanzlage und Kostenstruktur, z.B. dass As break-even-point für P bei n Euro liegt, und dass A nur einige Wochen lang Verluste verkraften kann. Es geht um nichttechnische Geschäftsgeheimnisse, die ausschließlich bei der Preisgestaltung eingesetzt werden können. Nun kann B gezielt „predatory pricing“-Taktiken einsetzen und P sogar defizitär verkaufen, um A vom Markt zu drängen.

Gemäß § 6 hätte A Anspruch auf Unterlassung der durch die widerrechtliche Geheimnisverwertung ermöglichten Handlung. Je nach Auslegung von § 7 Nr. 2 bis 5 i.V.m. § 2 Nr. 4 könnte A aber auch Anspruch auf den Rückruf und die Vernichtung des Produkts P haben,

<sup>8</sup> z.B. MPI Stellungnahme vom 3.6.2014, Rn. 22; GRUR Stellungnahme vom 19.3.2014, S. 5.

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 7|16

was deutlich über das Ziel der Richtlinie hinaus schießt. In diesen Fällen muss nach der vorliegenden Version des Gesetzestextes § 9 greifen, sodass Ansprüche auf Rückruf und Vernichtung des Produkts ausgeschlossen sind. Unterlassungsansprüche, gerichtet auf die durch die widerrechtliche Geheimnisverwertung ermöglichte Handlung, und Schadensersatzansprüche sind hier ausreichend. Soweit der Wortlaut nicht in einer Art und Weise geändert werden kann, die die aufgezeigte Lesart ausschließt, sollte zumindest eine entsprechende Auslegung in der Gesetzesbegründung vorgegeben werden.

### 3. Inhaberschaft und erlaubte Handlungen, § 2 Nr. 2 und § 3

Nach § 2 Nr. 2 kann jede natürliche oder juristische Person Inhaber eines Geschäftsgeheimnisses sein.

Während der Ref-E noch an eine rechtmäßige Erlangung und eine Nutzungs- und Offenlegungserlaubnis anknüpfte, übernimmt der Reg-E nahezu wortgleich den Richtlinienvorschlag und stellt auf die rechtmäßige Kontrolle über ein Geschäftsgeheimnis ab.

Bitkom begrüßt diese Änderung:

Nach der Begründung des Ref-E (S. 22) und Reg-E (S. 22. f.) sollte auch ein Lizenznehmer Inhaber eines Geschäftsgeheimnisses sein können. Fraglich ist hier, was mit einer Offenlegung im Falle eines Lizenznehmers gemeint ist und ob es sich tatsächlich um ein Geschäftsgeheimnis handeln kann, wenn eine Offenlegung erfolgt ist.

Nach Auffassung des Bitkom sollte es gerade keine Voraussetzung für die Inhaberschaft sein, ob der Inhaber das Geschäftsgeheimnis auch frei nutzen und offenlegen darf. Denn die Voraussetzungen der Nutzungs- und Offenlegungserlaubnis könnten im Einzelfall aufgrund z.B. vertraglicher Verpflichtungen (etwa durch die Vergabe eines ausschließlichen Nutzungsrechts durch den Inhaber an einen berechtigten Dritten) für den Inhaber nicht gegeben sein, was diesen aber nicht seiner Inhaberansprüche gem. §§ 6 ff. berauben sollte. Auch dürfte es nicht Ziel des Gesetzgebers sein, dem Lizenznehmer eine Inhaberschaft zu ermöglichen. Ob der Lizenznehmer auch Ansprüche nach §§ 6 ff. geltend machen kann, sollte zwischen den Parteien ausschließlich vertraglich vereinbart werden.

Was die Erlangung eines Geschäftsgeheimnisses betrifft, wird in § 3 Abs. 1 wie bereits im Ref-E mit Regelbeispielen näher definiert, wie Geschäftsgeheimnisse rechtmäßig erlangt werden dürfen. Unklar bleibt damit nach wie vor, welche weiteren Fälle es zum rechtmäßigen Erlangen des Geschäftsgeheimnisses geben könnte. Die aktuell offene Aufzählung birgt die Gefahr, dass sich der bereits bestehende Praxisstreit über die Inhaberschaft verschärft. Dies sollte dringend vermieden werden.

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 8|16

### Vorschlag zu § 3 Abs. 1:

„Ein Geschäftsgeheimnis darf **insbesondere** erlangt werden durch [...]“

Sinnvoll erscheint auch hier, sich näher an den Richtlinienvorgaben zu orientieren und die immerhin etwas konkretere, eingeschränkte Öffnungsklausel aus Art. 3 Abs. 1 d) der Richtlinie zu verwenden, nach der ein Erwerb bei „jede[r] anderen Vorgehensweise, die unter den gegebenen Umständen mit einer seriösen Geschäftspraxis vereinbar ist“, rechtmäßig ist. Auslegungshilfe zum Begriff der seriösen Geschäftspraxis bietet die ausdifferenzierte Rechtsprechung zur Sorgfalt eines ordentlichen Geschäftsmannes aus dem Gesellschaftsrecht.

### 4. Reverse Engineering, § 3 Abs. 1 Nr. 2

Anders als bisher im deutschen Recht wird das sog. Reverse Engineering nach § 3 Abs. 1 Nr. 2 grundsätzlich zulässig sein, es sei denn, vertragliche Abreden im Sinne einer „rechtsgültigen Pflicht“ aus Art. 3 Abs. 1 b) der Richtlinie stehen dem entgegen.

Aus Sicht des Bitkom ist die Einführung einer klaren Regelung für das Reverse Engineering zu begrüßen. Durch das Analysieren konkurrierender Produkte werden Innovationen gefördert und es erfolgt eine Angleichung insb. an die USA, wo Reverse Engineering von rechtmäßig erlangten Produkten schon lange als lauterer Verhalten gilt.<sup>9</sup> Wichtig ist dennoch, dass die Möglichkeit des vertraglichen Ausschlusses von Reverse Engineering bestehen bleibt, um den privatautonomen Entscheidungen der Teilnehmer am Wirtschaftsleben angemessen Rechnung zu tragen.

Die Zulässigkeit des Reverse Engineering ergab sich im deutschen Recht bisher nicht aus dem Gesetz. Im Gegenteil wurde beim Reverse Engineering häufig mit einer Verletzung von § 17 Abs. 1 Nr. 1 a) UWG („Anwendung technischer Mittel“) argumentiert. Das Merkmal „Anwendung technischer Mittel“ umfasst alle im weitesten Sinne der Technik zuzurechnenden Vorrichtungen, die der Erlangung oder Sicherung von Unternehmensgeheimnissen dienen können, wie etwa den Einsatz von Ablichtungsgeräten, Computern, Fotoapparaten und Filmkameras sowie das Abrufen von in Datenverarbeitungsanlagen gespeicherten Daten.<sup>10</sup> Oftmals wird sich beim Reverse Engineering genau solcher technischer Mittel bedient.<sup>11</sup>

<sup>9</sup> Vgl. [http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa\\_final\\_85.pdf](http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf), S. 5.

<sup>10</sup> Harte-Bavendamm/Henning-Bodewig/Harte-Bavendamm, UWG § 17 Rn. 22, mwN.

<sup>11</sup> Vgl. zum Streitstand *Kalbfus*, GRUR 2016, 1009, 1012.



## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 9|16

### 5. Handlungsverbote, § 4

§ 4 enthält Handlungsverbote. Er bedarf nach Auffassung des Bitkom keiner weiteren Anpassungen. Besonders § 4 Abs. 1 ist positiv hervorzuheben, in welchem die Vorgaben der Richtlinie in bekannte Termini aus dem deutschen Zivilrecht umgesetzt werden. So darf ein Geschäftsgeheimnis nach § 4 Abs. 1 Nr. 2 nicht durch „*jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheiten entspricht*“ erlangt werden.

Die Grundsätze von Treu und Glauben nach § 242 BGB, zu denen es eine Reihe von Rechtsprechung gibt, führen zu Rechtssicherheit. Auch den Begriff der „*anständigen Marktgepflogenheiten*“ kennt das deutsche Recht bereits. Im UWG wird in § 2 Abs. 1 Nr. 7 die „*unternehmerische Sorgfalt*“ als „*der Standard an Fachkenntnissen und Sorgfalt, von dem billigerweise angenommen werden kann, dass ein Unternehmer ihn in seinem Tätigkeitsbereich gegenüber Verbrauchern nach Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheiten einhält*“, definiert.

Zudem kann zur Auslegung des so formulierten Auffangtatbestandes die Fußnote 10 zu Art. 39 Abs. 2 TRIPS herangezogen werden. Danach sollen unseriöse Geschäftspraktiken wenigstens solche sein, die einen Vertragsbruch, den Bruch einer Vertraulichkeitsvereinbarung oder die Anstiftung zu einem solchen Bruch herbeiführen, sowie der Erwerb geheimer Information durch Dritte, die zum Zeitpunkt des Erwerbs wussten oder grob fahrlässig nicht wussten, dass unseriöse Geschäftspraktiken an dem Erwerb angewendet wurden.<sup>12</sup>

### 6. Rechtfertigungsgründe, § 5

§ 5 enthält Rechtfertigungsgründe. Dabei macht der Gesetzesentwurf den Rechtfertigungsgrund des „*berechtigten Interesses*“ aus Art. 5 d) der Know-how-Richtlinie zum Oberbegriff und die Nr. 1 bis 3 zu Fällen desselben, was zwar mit der formalen Systematik des Art. 5 der Know-how-Richtlinie bricht, mit dem Leitgedanken dieses Artikels aber vereinbar erscheint.

<sup>12</sup> Vgl. Koós, MMR, 2016, 224; TRIPS-Fußnote: [https://www.wto.org/english/docs\\_e/legal\\_e/27-trips\\_04d\\_e.htm](https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm).

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 10|16

*Die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses ist gerechtfertigt, wenn dies zum Schutz eines berechtigten Interesses erfolgt, insbesondere*

*1. zur Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit nach der Charta der Grundrechte der Europäischen Union, einschließlich der Achtung der Freiheit und der Pluralität der Medien;*

*2. zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die das Geschäftsgeheimnis erlangende, nutzende oder offenlegende Person in der Absicht handelt, das allgemeine öffentliche Interesse zu schützen;*

*3. im Rahmen der Offenlegung durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn dies erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann.*

Zu begrüßen ist, dass durch diese Struktur der Schrankenregelung eine Interessenabwägung im Einzelfall zu erfolgen hat („zum Schutz eines berechtigten Interesses erforderlich“). Was in der so gefassten deutschen Umsetzung bisher jedoch im Gesetzestext selbst fehlt, ist der ausdrückliche Hinweis auf *nach geltendem Recht* anerkannte Interessen („durch das Unionsrecht oder das nationale Recht anerkannten legitimen Interesses“, Art. 5 d) der Richtlinie). Die Einleitung des § 5 sollte diese Formulierung zur Klarstellung beinhalten.

### Vorschlag zu § 5 Satz 1:

*„Die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses ist gerechtfertigt, wenn dies zum Schutz eines **berechtigten nach geltendem Recht anerkannten** Interesses erforderlich ist, insbesondere (...).“*

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 11|16

### 6.1 Meinungsäußerungs- und Informationszugangsfreiheit, Pluralität der Medien, § 5 Nr. 1

Die Schrankenregelung in § 5 Nr. 1 hat insbesondere für investigativen Journalismus eine große Bedeutung. Es sollte sichergestellt werden, dass die Schranke nur greift, wenn das Interesse an der Ausübung des Rechts der freien Meinungsäußerung das berechnete Interesse des Geheimnisinhabers an der Verhinderung der Veröffentlichung wesentlich überwiegt. Die Ausübung der Meinungs- und Informationsfreiheit muss immer in einem angemessenen Verhältnis zum berechtigten Interesse des Geschäftsgeheimnisträgers stehen. Nur in besonderen Ausnahmefällen kann die Informations-, Meinungsäußerungs- oder Pressefreiheit tatsächlich überwiegen.

### 6.2 Whistleblowing, § 5 Nr. 2

Der Gesetzesentwurf sieht in Umsetzung der Richtlinie in § 5 Nr. 2 eine Privilegierung von Whistleblowing vor. Nach Ansicht des Bitkom mündet die konkrete Ausgestaltung der – grundsätzlich begrüßenswerten – Neuerung jedoch in einer ungerechtfertigten Benachteiligung der Unternehmerseite. Es mangelt an einer Pflicht zur abgestuften Vorgehensweise. Diese sollte eingefügt werden, um Unternehmen die „ultima ratio“ in Gestalt von Presseartikeln zu ersparen, welche in massiven Rufschäden enden können, ohne dass dies in jedem Fall verhältnismäßig zur Schwere des Verstoßes wäre.

Vorschlag zu § 5 Nr. 2:

„(...) zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die das Geschäftsgeheimnis erlangende, nutzende oder offenlegende Person **zuvor erfolglos unternehmensintern im Rahmen des Zumutbaren Abhilfe verlangt hat und** in der Absicht handelt, das allgemeine öffentliche Interesse zu schützen;“

Nach bisheriger Rechtslage war ein Whistleblower im Rahmen des § 17 UWG bei Vorliegen der Voraussetzungen des rechtfertigenden Notstands nach § 34 StGB straffrei, sofern der Geheimnisverrat zur Abwendung einer gegenwärtigen Gefahr für ein höherrangiges eigenes oder fremdes Rechtsgut erfolgte. Allerdings kam eine Rechtfertigung nur in Betracht, wenn mildere Mittel zum Schutz des höherrangigen Rechtsguts nicht greifbar waren. Beispielsweise konnte das Offenlegen einer vertraulichen Information gerechtfertigt sein, wenn sie eine rechtswidrige Handlung betraf, die anderweitig nicht aufgedeckt werden konnte und ihre Offenlegung einen Beitrag zum geistigen Meinungskampf in der Öffent-

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 12|16

lichkeit darstellte.<sup>13</sup> Allerdings stand es einer Rechtfertigung gem. § 34 StGB regelmäßig entgegen, wenn der Whistleblower die Presse informierte, anstatt sich an die Strafverfolgungsbehörden zu wenden, oder wenn er die Information aus Gewinnerzielungsinteresse weitergab und daher das Vorliegen subjektiver Rechtfertigungselemente fraglich war. Auch durfte das Strafverfolgungsinteresse nicht pauschal als gegenüber dem Geheimhaltungsinteresse höherrangig eingestuft werden, vielmehr kam es auf die Schwere der Straftat an.<sup>14</sup>

Bitkom steht dem Schutz von Whistleblowern positiv gegenüber. Jedoch geht der Gesetzesentwurf über den sinnvollen, von der Rechtsprechung statuierten Grundsatz des zunächst innerbetrieblichen Abhilfeversuchs hinaus. Nach diesem ist es einem Arbeitnehmer grundsätzlich zuzumuten, den angezeigten Missstand zunächst innerbetrieblich anzuzeigen und zu klären. Als Ausfluss der Treue- und Loyalitätspflicht des Arbeitnehmers nach § 241 Abs. 2 BGB bzw. bei Beamten nach § 125 Abs. 1 S. 2 BBG müssen Informationen zunächst dem Vorgesetzten gegeben werden und nur wenn dies unmöglich oder unzumutbar ist, kann der Arbeitnehmer als letzte Option damit an die Öffentlichkeit gehen.<sup>15</sup> Nach dem Referenten- und nunmehr dem Regierungsentwurf sind Hinweisgeber hingegen nicht verpflichtet, ein solches Abhilfegesuch zu unternehmen.

Auch ist der Adressatenkreis etwaiger Berichte über unternehmensinterne Missstände nicht beschränkt: Der Whistleblower kann entscheiden, ob er sich an bestimmte Behörden wendet oder direkt an die Öffentlichkeit bzw. die Medien. Der Gesetzesentwurf spricht lediglich von der „Aufdeckung“ eines Fehlverhaltens. Eine nähere Spezifikation, wie etwa in § 17 Abs. 2 Arbeitsschutzgesetz, wonach sich Beschäftigte nach erfolglosem, betriebsinternen Abhilfebegehren an die zuständige Behörde zu wenden haben, sieht die Richtlinie nicht vor.

Die entworfene Regelung bleibt auch hinter dem von der EU Kommission am 23. April 2018 veröffentlichten Entwurf einer Richtlinie zum Schutz von Whistleblowern zurück. Danach sollen gerade interne und externe Meldekanäle, Art. 3 Nr. 6, 7 COM(2018) 218 final, und Verfahren, Art. 4 ff. COM(2018) 218 final, durchlaufen werden, bevor ein Whistleblower an die Öffentlichkeit gehen darf. Die Mitteilung an die Medien soll auch hier – wie bisher beim innerbetrieblichen Abhilfeversuch – die „ultima ratio“ sein. Die Möglichkeit für Unternehmen, solche Stufenprozesse zu etablieren, entspricht ihrem Interesse daran, sich zunächst intern mit den Vorwürfen auseinanderzusetzen. Denn auch das Unternehmen selbst hat ein Interesse daran, Fehlverhalten schnellstmöglich zu erkennen und Fehler abzustellen. Hatte ein Unternehmen bis zu dem Zeitpunkt selbst keine positive

<sup>13</sup> OLG München, GRUR-RR 04, 145, 146f.

<sup>14</sup> *Ohly/Sosnitza/Ohly*, UWG § 17 Rn. 30, m.w.N.

<sup>15</sup> Vgl. auch *Eufinger*, ZRP, 2016, 229.

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 13|16

Kenntnis, muss ihm aber die Möglichkeit eingeräumt werden, sich damit intern auseinanderzusetzen und selbst entsprechend zu reagieren, bevor etwas an die Öffentlichkeit gegeben wird. Nur so kann einer womöglich nicht gerechtfertigten Rufschädigung eines Unternehmens begegnet und ein möglicher Schaden effektiv abgewendet werden.

Hinsichtlich der Richtlinie zum Schutz von Whistleblowern ist schließlich noch zu beachten, dass Unternehmen nach Umsetzung jener Richtlinie in naher Zukunft zu weiteren betrieblichen Anpassungen an die kommende Gesetzeslage gezwungen sein werden. Durch die fragwürdige Vorgehensweise, einen abgrenzbaren Themenkreis häppchenweise, statt in einem Zuge zu regeln, werden der Wirtschaft ohne Not Kosten aufgebürdet und es leidet die Verständlichkeit des Rechts: Eine Stückelung der Kodifizierung von Whistleblowing als Rechtfertigungsgrund über zwei Regelwerke (§ 5 Nr. 2 Reg-E und Art. 15 Nr. 7 der Whistleblower-Richtlinie) wäre vermeidbar gewesen. Die Implementierung eines solchen Stufenprozesses muss sich auch auf den Schutzbereich in §§ 2 bis 4 GeschGehG-E auswirken, damit ein Anreiz für solche unternehmensinternen Investitionen geschaffen wird.

### 7. Ansprüche bei Rechtsverletzungen

Gem. § 9 sind Ansprüche nach §§ 6 bis 8 ausgeschlossen,

*„wenn die Erfüllung im Einzelfall unverhältnismäßig wäre unter Berücksichtigung insbesondere*

*(...)*

*2. der getroffenen Geheimhaltungsmaßnahmen;“*

Angemessene Geheimhaltungsmaßnahmen sind jedoch bereits eine notwendige Voraussetzung für das Vorliegen eines Geschäftsgeheimnisses gemäß § 2 Nr. 1. Eine erneute Prüfung im Rahmen des Verhältnismäßigkeitseinwands nach § 9 erscheint überflüssig und systematisch verfehlt.

### 8. Verfahrensrechtlicher Geheimnisschutz

Für einen effektiven Schutz von Geschäftsgeheimnissen muss der Schutz auch auf verfahrensrechtlicher Ebene gewährleistet sein. So setzen die §§ 15 bis 22 den Art. 9 der Richtli-

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 14|16

nie um und regeln den Schutz von Geschäftsgeheimnissen während des Gerichtsverfahrens.

Bitkom hält die insoweit bisher im GeschGehG-E gefundenen Regelungsansätze für vertretbar und begrüßt besonders die im Bereich der Ordnungsmittel neu festgelegten Größenordnungen. Generellen Handlungsbedarf sehen wir noch im Bereich der Datensicherheit im Gerichtsverkehr.

Der Geschäftsgeheimnisschutz im Verfahren war im deutschen Recht bislang nur lückenhaft geregelt, vgl. etwa § 172 Nr. 2 GVG, § 384 ZPO. Die Schwierigkeit liegt darin, dass während eines Prozesses einerseits sichergestellt sein muss, dass das Geheimnis nicht der Öffentlichkeit oder (potenziellen) Wettbewerbern offenbart und somit ein Verletzungsverfahren zur Ausforschung missbraucht wird. Andererseits sind die zivilprozessrechtlichen Grundsätze der Öffentlichkeit, Mündlichkeit und Unmittelbarkeit zu wahren.

In § 172 Nr. 2 GVG ist die Möglichkeit vorgesehen, die Öffentlichkeit auszuschließen, sofern ein wichtiges Geschäfts-, Betriebs-, Erfindungs- oder Steuergeheimnis zur Sprache kommt, durch dessen öffentliche Erörterung überwiegende schutzwürdige Interessen verletzt würden (Ermessensentscheidung durch das Gericht<sup>16</sup>). Dadurch kann aber nur die Öffentlichkeit ausgeschlossen werden, nicht die andere Vertragspartei. Zudem betrifft es nur die mündliche Verhandlung bzw. Teile von dieser und nicht den gesamten Rechtsstreit. Ein Ausschluss kann nur dann erfolgen, wenn ein wichtiges Geheimnis thematisiert wird, wodurch der Anwendungsbereich weiter verengt wird.<sup>17</sup>

In Patentstreitigkeiten wird das o.g. Dilemma in Deutschland durch das sog. „Düsseldorfer Verfahren“ gelöst, das in der Studie zur Vorbereitung der Richtlinie positiv als effektiver Schutzmechanismus hervorgehoben wurde. Beim Düsseldorfer Beweisverfahren handelt es sich um ein verfahrensrechtliches Hybrid aus einem selbstständigen Beweis- und einem einstweiligen Verfügungsverfahren. Es trägt dem Problem Rechnung, dass die Auskunftspflicht gerade der Feststellung der Verletzung dient, der angebliche Verletzer hierzu aber sensible Informationen offenlegen müsste. Drei Sicherungsmechanismen sollen verhindern, dass eine Verletzungsklage zu Ausforschungszwecken missbraucht wird: Erstens wird die Durchsetzung des Informationsanspruchs in ein selbstständiges Beweisverfahren vorverlagert, dessen Entscheidung im Vorfeld des Hauptprozesses im Rechtsmittelweg überprüft werden kann. Zweitens wird das Geheimnis vorerst nur einem Sachverständigen zugänglich gemacht, der ein Gutachten erstellt, das dem Gericht und ausgewählten Prozessvertretern, nicht aber der gegnerischen Partei, vorgelegt wird. Auf Basis dieses Gut-

<sup>16</sup> Götz, Der Schutz von Betriebs- und Geschäftsgeheimnissen im Zivilverfahren, 2014, S. 201.

<sup>17</sup> Vgl. McGuire; GRUR 2015, 424, 428.

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 15|16

achdens beurteilt das Gericht, ob eine hohe Verletzungswahrscheinlichkeit vorliegt. Nur wenn dieser strenge Maßstab erfüllt ist, kann die Information für den Gegner freigegeben werden. Drittens macht sich die Gegenpartei schadensersatzpflichtig, wenn sie die Freigabe durchsetzt, sich anschließend aber herausstellt, dass keine Verletzung vorlag.<sup>18</sup>

Die Etablierung eines sog. in-camera Verfahrens findet in der Richtlinie keine Erwähnung, wurde aber während des Gesetzgebungsverfahrens diskutiert. Bei einem solchen Geheimverfahren werden die zu schützenden Informationen nur dem Gericht vollständig vorgelegt, nicht aber der Gegenseite.<sup>19</sup> Im deutschen Recht ist ein in-camera Verfahren im Zivilprozess bislang ebenfalls nicht vorgesehen. Denn der Prozessgegner hat bei einem solchen Verfahren nicht die Möglichkeit, Kenntnis von allen entscheidungserheblichen Tatsachen zu nehmen und kann die Angaben der gegnerischen Partei nicht selbst nachprüfen. Dies ist zivilprozessual im Hinblick auf den Unmittelbarkeits- und Mündlichkeitsgrundsatz aus § 128 ZPO und dem Anspruch auf rechtliches Gehör und ein faires Verfahren problematisch.

Zu verfahrensrechtlichen Einzelheiten im GeschGehG-E ist anzumerken:

Die in § 15 Abs. 1 normierte sachlich ausschließliche Zuständigkeit der Landgerichte ohne Rücksicht auf den Streitgegenstand bewerten wir positiv.

Gem. § 16 kann das Gericht auf Antrag einer Partei streitgegenständliche Informationen ganz oder teilweise als geheimhaltungsbedürftig einstufen, wenn diese ein Geschäftsgeheimnis sein können. Gem. § 19 Abs. 1 kann das Gericht dabei auf Antrag einer Partei den Kreis der Personen, die Zugang zu den Informationen haben werden, auf eine bestimmte Anzahl von Personen beschränken sowie nach Abs. 2 Nr. 1 die Öffentlichkeit ausschließen. Diese Regelungen sind zur Sicherung von Geschäftsgeheimnissen ebenfalls sinnvoll und sollten beibehalten werden.

Nach § 17 zieht eine Zuwiderhandlung gegen § 16 Abs. 2 ein Ordnungsgeld von nunmehr bis zu 100.000,- € oder Ordnungshaft bis zu sechs Monaten nach sich. Bitkom begrüßt die Anhebung des Ordnungsmittelrahmens auf ein spürbares Niveau als einen Schritt in die richtige Richtung. Den Richtlinienvorgaben aus Art. 16 über wirksame, verhältnismäßige und abschreckende Sanktionen wird nunmehr besser Genüge getan. Der noch im Ref-E angesetzte Rahmen von nur 1.000,- € bzw. Ordnungshaft von bis zu sechs Wochen war im Verhältnis zu den denkbaren hochwertigen Streitgegenständen eindeutig nicht hinrei-

<sup>18</sup> GRUR 2015, 424; zum Verfahren im Allgemeinen vgl. auch [http://www.grur.org/uploads/tx\\_meeting/Vortrag\\_Dr\\_Deichfuss.pdf](http://www.grur.org/uploads/tx_meeting/Vortrag_Dr_Deichfuss.pdf).

<sup>19</sup> siehe ausführlich dazu *McGuire*

[http://www.grur.org/uploads/tx\\_meeting/Vortrag\\_Prof\\_Mc\\_Guire\\_mit\\_Handouts\\_01.pdf](http://www.grur.org/uploads/tx_meeting/Vortrag_Prof_Mc_Guire_mit_Handouts_01.pdf).

## Stellungnahme Umsetzung Know-how-Richtlinie

Seite 16|16

chend und keinesfalls abschreckend. Schon aus Gründen der Generalprävention sollte die Grenze nicht zu niedrig angesetzt werden.

Für einen weiten Ordnungsmittelrahmen spricht schließlich auch folgender Gedanke: Sollte sich eine geheimhaltungsbedürftige Information im Nachhinein nicht als Geschäftsgeheimnis erweisen, fällt der von § 10 und § 23 vorgesehene zivil- und strafrechtliche Schutz weg. Es bleibt allein § 17. Um dennoch einen effektiven Schutz zu gewährleisten, ist es erforderlich, hinreichend abschreckende Ordnungsmittel vorzuhalten.

Zur generellen Frage der Datensicherheit im Gerichtsbetrieb ist festzustellen, dass alle Verfahrensbeteiligten eine entsprechende Fachkunde für den Umgang mit geheimhaltungsbedürftigen Informationen besitzen sollten. Diese sollte durch Rechtsverordnung geregelt werden. Insbesondere Rechtspfleger sollten wissen, wie wirksam verschlüsselt wird (Umgang mit Tools), was Social Engineering und wie Datensicherheit zu gewährleisten ist. Hier sieht Bitkom weiteren Handlungsbedarf.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.