

Die neue EU-Know-How-Schutz-Richtlinie - Executive Summary



Von Vera Buriánek

Die Frist zur Umsetzung der EU-„Know-How-Schutz-Richtlinie“¹ durch den Gesetzgeber lief am 9. Juni 2018 ab. Sie bietet einerseits den Vorteil zeitlich unbegrenzten und EU-weiten Schutzes, stellt andererseits die Schutzworaussetzung unternehmensweiter Geheimhaltungsmaßnahmen für Know-How auf.

I. Was wird geschützt (Schutzobjekt)?

Die Richtlinie stellt einen verbindlichen Mindeststandard für den Schutz von Know-How durch alle EU-Mitgliedstaaten auf.

Zunächst führt die Richtlinie eine EU-weit einheitliche Definition für vertrauliches Know-how, sog. Geschäftsgeheimnisse, ein:

„...der Ausdruck 'Geschäftsgeheimnis' (bezeichnet) Informationen, die alle nachstehenden Kriterien erfüllen:

a) Sie sind in dem Sinne geheim, dass sie weder in ihrer Gesamtheit 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 sind;

b) sie sind von kommerziellem Wert, weil sie geheim sind;

c) sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt;“

(Artikel 2 Nr.1 Richtlinie)

Diese Definition stimmt sowohl mit jener aus Artikel 39 Abs. 2 TRIPS-Abkommen² als auch mit der in 48 von 50 US-Staaten anwendbaren Begriffsbestimmung überein. Als „Geschäftsgeheimnis“ in diesem Sinne kommen in der Praxis eine ganze Bandbreite an Informationen in Frage: „technologische(s) Wissen ... und ... Geschäftsdaten wie Informationen über Kunden und Lieferanten, Businesspläne sowie Marktforschung und -strategien“ (Richtlinie, Erwägungsgrund 2) sind von diesem Begriff umfasst.

Ein aktueller Entwurf für das deutsche Umsetzungsgesetz zur Richtlinie führt darüber hinaus Forschungsergebnisse von Universitäten (wenn diese am Wettbewerb teilnehmen), Herstellungsverfahren, Kunden- und Lieferanten-

listen, Kosteninformationen, Geschäftsstrategien, Unternehmensdaten, Marktanalysen, Prototypen, Formeln und Rezepte auf.

Die beiden entscheidenden Voraussetzungen für die Schutzfähigkeit von Informationen dieser Art als „Geschäftsgeheimnis“ sind, (a) dass sie geheim sind und (b) dass „angemessene Geheimhaltungsmaßnahmen“ durch die rechtmäßig über die Informationen Verfügenden getroffen werden. Die dritte in der Richtlinie genannte Voraussetzung des tatsächlichen oder potenziellen Wertes der Informationen, gerade (auch) wegen ihres geheimen Charakters, sollte sich in der Praxis nicht auswirken.

II. Wer wird geschützt? (Schutzsubjekt)

Die Richtlinie schützt Unternehmen, die über Geschäftsgeheimnisse verfügen, unabhängig von ihrer Organisationsform, ihrer Größe, ihres Marktanteils oder ihres Geschäftsfelds, einschließlich Start-ups, KMUs und nichtkommerzielle Forschungseinrichtungen.

III. Schutz wovor? (Verletzungshandlungen)

Artikel 4 Absatz 2 (a) der Richtlinie stuft „unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren

von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle durch den Inhaber des Geschäftsgeheimnisses unterliegen..." als rechtswidrig ein.

Darüber hinaus umfasst der weite Auffangtatbestand in Artikel 4 Absatz 2 (b) „jedes sonstige Verhalten, das unter den jeweiligen Umständen als mit einer seriösen Geschäftspraxis nicht vereinbar gilt“. Nach der Gesetzesbegründung zum deutschen Umsetzungsgesetz, ist der Begriff „seriöse Geschäftspraxis“ aus Fußnote 10 zu Artikel 39 Absatz 2 TRIPS-Abkommen heraus zu definieren. Darin heißt es:

„10. Für die Zwecke dieser Bestimmung bedeutet "eine Weise, die den anständigen Gepflogenheiten im Gewerbe und Handel zuwiderläuft" zumindest Handlungen wie Vertragsbruch, Vertrauensbruch und Verleitung dazu und schließt den Erwerb nicht offenbarter Informationen durch Dritte ein, die wussten oder grob fahrlässig nicht wussten, dass solche Handlungen beim Erwerb eine Rolle spielten.“³

Im Gegensatz zum bisherigen Geschäftsgeheimnis-Schutz durch das deutsche „Gesetz gegen den unlauteren Wettbewerb“, wird „Reverse Engineering“ des Inhalts des Geschäftsgeheimnisses in der Richtlinie nicht mehr als rechtswidrig eingestuft,⁴ solange dadurch nicht gleichzeitig eine „Vertraulichkeitsvereinbarung oder eine

sonstige Verpflichtung, das Geschäftsgeheimnis nicht offenzulegen“, Artikel 4 Nr. 2 (b) Richtlinie, verletzt wird.

IV. Rechtsbehelfe gegen Verletzungen

Bei Verletzung von Geheimnisschutz-Rechten stehen betroffenen Unternehmen gemäß Artikel 12 Richtlinie die folgenden Maßnahmen zu Verfügung: (a) Unterlassungsverfügung bzw. gerichtliches Verbot der rechtswidrigen Nutzung/Offenlegung des Geschäftsgeheimnisses; (b) Verbot des Herstellens, Anbietens, Vermarktens oder der Nutzung rechtverletzender Produkte und der Einfuhr, Ausfuhr oder Lagerung rechtsverletzender Produkte für solche Zwecke; Zerstörung oder Herausgabe der rechtsverletzenden Gegenstände an den Antragsteller oder an wohltätige Organisationen (c) „Zwangmaßnahmen“ wie Rückruf oder Zerstörung der verletzenden Produkte sowie (d) Veröffentlichung der Gerichtsentscheidung mit öffentlicher Klarstellung, dass ein Geschäftsgeheimnis verletzt wurde.

V. Schutzdauer/Rechtsbehelfe

Die Schutzdauer von Geschäftsgeheimnissen ist unbegrenzt und hängt allein davon ab, ob die jeweilige Information weiterhin „geheim“ im Sinne der Richtlinie ist. Rechtsbehelfe auf Grundlage der Richtlinie dürfen im nationalen Umsetzungsgesetzen keiner längeren Verjährungsfrist als sechs Jahre unterliegen, vgl. Artikel 8 Richtlinie. Der deutsche Gesetzes-

entwurf für ein Umsetzungsgesetz wendet die Regelverjährungsfrist im Zivilrecht von drei Jahren auf Verletzungen des Geschäftsgeheimnisschutzes an.

VI. Ausnahmen vom Schutzbereich

Wichtigste Ausnahme vom Geschäftsgeheimnis-Schutzregime der Richtlinie ist jene für Whistleblowing: Solange der Whistleblower

„zur Aufdeckung eines beruflichen oder sonstigen Fehlverhaltens oder einer illegalen Tätigkeit, sofern der Antragsgegner in der Absicht gehandelt hat, das allgemeine öffentliche Interesse zu schützen;“ (Art. 5 (b) Richtlinie),

greift kein Geschäftsgeheimnis-Schutz, Rechtsbehelfe nach den jeweiligen nationalen Umsetzungsgesetzen bleiben erfolglos.

Die Gesetzesbegründung zum deutschen Gesetzesentwurf für ein Umsetzungsgesetz definiert den zentralen Begriff des „Fehlverhalten“ näher. Ein solches umfasse über rechtswidriges Verhalten hinaus unethisches Verhalten und nennt durch Whistleblowing aufgedeckte Auslandsaktivitäten eines Unternehmens, die in den jeweiligen Ländern nicht rechtswidrig sind, jedoch von der öffentlichen Meinung als Fehlverhalten angesehen werden könnten, wie beispielsweise Kinderarbeit oder gesundheits-/umweltschädliche Produktionsbedingungen oder systematische Umgehung von Steuertatbeständen.

Weitere Informationen:

Meissner Bolte – Vera Buriánek – Widenmayerstrasse 47, 80538 München, Deutschland
Telefon +49-89-21 21 86-0, Fax +49-89-21 21 86-70, E-mail: mail@mb.de, www.mb.de

Die in diesem Newsletter enthaltenen Informationen geben die bei Veröffentlichung bekannten neuesten rechtlichen Entwicklungen wieder. Es wird jedoch darauf hingewiesen, dass keine Garantie für die Richtigkeit und Vollständigkeit übernommen wird. Diese Informationen stellen keine Hinweise für künftige Ergebnisse dar und sollen nicht als solche angesehen werden. Meissner Bolte weist ausdrücklich darauf hin, dass keine Haftung für vorgenommene oder unterlassene Aktivitäten aufgrund der in dem Newsletter enthaltenen Informationen übernommen wird.



VII. Vorbereitung von Unternehmen auf die neue Richtlinie („angemessener Geheimhaltungsmaßnahmen“)

Die Richtlinie stellt als Schutzvoraussetzung das Erfordernis „angemessene Geheimhaltungsmaßnahmen“ durch das jeweilige Unternehmen auf, Artikel 2 Nr. 1 c Richtlinie. Deshalb sollten Inhaber von Geschäftsgeheimnissen ein solches Maßnahmenprogramm in ihrem Geschäftsbetrieb umsetzen. Nachdem bislang Rechtsprechung zum Umfang „angemessener“ Geheimhaltungsmaßnahmen fehlt, ist es kaum absehbar, wie Gerichte diesen Begriff in Zukunft auslegen werden.

Die Gesetzesbegründung zum Entwurf eines deutschen Umsetzungsgesetzes nennt lediglich relevante Faktoren für die Bewertung der „Angemessenheit“ von Geheimhaltungsmaßnahmen: der Wert des Geschäftsgeheimnisses, dessen Entwicklungskosten, die Bedeutung für das Unternehmen, die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen, die Art der Kennzeichnung der Informationen (z.B. als „vertraulich“) und vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern.

VIII. Mögliche Schutzmaßnahmen für Geschäftsgeheimnisse

a) Zugangsbeschränkungen auf einzelne Personen sowohl im „gegenständlichen“ Geschäftsbetrieb als

auch in der digitalen Unternehmenssphäre

b) systematische Einordnung und Kennzeichnung von „gegenständlichen“ und digitalen Arbeitsmitteln nach „Vertraulichkeitsstufen“ (z.B: öffentlich, vertraulich, streng vertraulich); Arbeitsprozesse auf „need to know“-Basis organisieren, wo potenzielle Geschäftsgeheimnisse betroffen sein können

c) Unternehmensrichtlinie zur Vertraulichkeit einführen, indem klare Verhaltensstandards für Mitarbeiter bzgl. Behandlung sensibler Geschäftsinformationen aufgestellt und an die Belegschaft kommuniziert werden;

d) IT-Sicherheit im Unternehmen überprüfen, insbesondere im Hinblick auf Risiken des Datendiebstahls von außen durch Hacker

e) bestehende Verträge auf „Geheimhaltungsklauseln“/ Wettbewerbsverbote überprüfen und ggf. solche neu aufnehmen

➤ Arbeitsverträge, Geheimhaltungsvereinbarungen und nachvertragliche Wettbewerbsverbote mit Mitarbeitern (innerhalb der Grenzen des zulässigen, was räumlichen und zeitlichen Umfang des Wettbewerbsverbots betrifft)

➤ Verträge mit Geschäftspartner (insbesondere Zulieferern) sollten außer Vertraulichkeitsvereinbarungen auch „limited use“-Klauseln in

Bezug auf Unternehmenserzeugnisse beinhalten, um (zukünftig legales) Reverse Engineering vertraglich zu unterbinden

f) Geschäftsgeheimnisschutz-Verletzungen durch neu eingestellte Mitarbeiter verhindern im Umkehrschluss: zum Schutz eigener Geschäftsgeheimnisse durch die Richtlinie ist auch auf die Vermeidung von Know-how-Schutzverletzungen Dritter im eigenen Unternehmen zu achten, insbesondere durch neue Mitarbeiter. Dazu kann eine Standard-Klausel in die Arbeitsvertragsmuster eingefügt werden, die neue Arbeitnehmer auf Risiken im Hinblick auf die Offenbarung von Geschäftsgeheimnissen des früheren Arbeitgebers aufmerksam macht.

g) Schriftliche Dokumentation aller umgesetzten Geheimschutzmaßnahmen

Schließlich sollten alle umgesetzten Maßnahmen dokumentiert werden, um im Streitfall den Beweis über „abgemessene Geheimhaltungsmaßnahmen“ erbringen zu können. Darüber hinaus sollte überlegt werden, den konkreten Wert einzelner wichtiger Geschäftsgeheimnisses in der Unternehmensbilanz zu berücksichtigen und damit zu beziffern⁵, denn dies hilft im Streitfall bei der Bezifferung eines etwaigen Schadensersatzes.

Weitere Informationen:

Meissner Bolte – Vera Buriánek – Widenmayerstrasse 47, 80538 München, Deutschland
Telefon +49-89-21 21 86-0, Fax +49-89-21 21 86-70, E-mail: mail@mb.de, www.mb.de

Die in diesem Newsletter enthaltenen Informationen geben die bei Veröffentlichung bekannten neuesten rechtlichen Entwicklungen wieder. Es wird jedoch darauf hingewiesen, dass keine Garantie für die Richtigkeit und Vollständigkeit übernommen wird. Diese Informationen stellen keine Hinweise für künftige Ergebnisse dar und sollen nicht als solche angesehen werden. Meissner Bolte weist ausdrücklich darauf hin, dass keine Haftung für vorgenommene oder unterlassene Aktivitäten aufgrund der in dem Newsletter enthaltenen Informationen übernommen wird.



Quellen:

¹ : Richtlinie EU) 2016/943 des Europäischen Parlaments 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, Volltext abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L0943&from=DE>.

² : Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen

Eigentums (= Agreement on Trade-Related Aspects of Intellectual Property Rights, "TRIPS") zwischen allen Mitgliedstaaten der WTO, englischsprachiger Volltext abrufbar unter: https://www.wto.org/english/docs_e/le-gal_e/31bis_trips_04d_e.htm.

³ : Deutschsprachige Fassung des TRIPS-Abkommens der „Bekanntmachung zu dem Übereinkommen über handelsbezogene Aspekte des geistigen Eigentums“ vom 15.04.1994, BGBl. II, S. 1730 ff.

⁴ : Köhler/Bornkamm/Feddersen/Köhler, UWG, §§ 17-19, Rn. 17; Steinmann/Schubmehl, Vertraglicher Geheimnisschutz im Kunden-Lieferanten-Verhältnis – Auswirkungen der EU-Geheimnisschutz-RL am Beispiel der Automobilindustrie, CCZ, 194.

⁵ : Hoeren/Münker, Die EU-Richtlinie für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung – unter besonderer Berücksichtigung der Produzentenhaftung, WRP 2018, 150, 151.

Weitere Informationen:

Meissner Bolte – Vera Buriánek – Widenmayerstrasse 47, 80538 München, Deutschland
Telefon +49-89-21 21 86-0, Fax +49-89-21 21 86-70, E-mail: mail@mb.de, www.mb.de

Die in diesem Newsletter enthaltenen Informationen geben die bei Veröffentlichung bekannten neuesten rechtlichen Entwicklungen wieder. Es wird jedoch darauf hingewiesen, dass keine Garantie für die Richtigkeit und Vollständigkeit übernommen wird. Diese Informationen stellen keine Hinweise für künftige Ergebnisse dar und sollen nicht als solche angesehen werden. Meissner Bolte weist ausdrücklich darauf hin, dass keine Haftung für vorgenommene oder unterlassene Aktivitäten aufgrund der in dem Newsletter enthaltenen Informationen übernommen wird.

