Blickpunkt Brüssel

Whitepaper: Der effektive Schutz von Geschäftsgeheimnissen in Europa

Sebastian Klein

Mai

2019

I. Kernpunkte

Am 5. Juli 2016 ist die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen[1] EU-weit in Kraft getreten. Sie hat wesentliche Veränderungen für den Geschäftsgeheimnisschutz mit sich gebracht, die bereits heute für alle Unternehmen in der Europäischen Union Wirkung entfalten. Um den neuen Möglichkeiten, Gefahren und Anforderungen der Richtlinie zu begegnen, besteht dringender Handlungsbedarf, denn:

1. Nach der Richtlinie sind nunmehr nur solche Informationen als Geschäftsgeheimnis geschützt, die Gegenstand angemessener Geheimhaltungsmaßnahmen sind. Diese Anforderung dürfte die weitreichendste Neuerung der Richtlinie darstellen und macht einen effektiven Geschäftsgeheimnisschutz im Unternehmen unabdingbar. Nur solche Unternehmen, die ausreichende organisatorische, vertragliche und technische Maßnahmen getroffen haben, um ihre Geschäftsgeheimnisse zu schützen, können gerichtlich gegen die Verletzung von Geschäftsgeheimnissen vorgehen.

2. Dies bringt ein nicht zu unterschätzendes Haftungsrisiko für das Management des Unternehmens mit sich. Sollte sich in einem Prozess herausstellen, dass das Management keine angemessenen Maßnahmen getroffen hat, um die Geheimnisse des Unternehmens wirksam zu schützen, kann das Management unter Umständen für den Verlust des gerichtlichen Schutzes verantwortlich gemacht werden.

3. In der Vergangenheit war lange unklar, ob „Reverse Engineering" eine Verletzung von Geschäftsgeheimnissen darstellt. Diese Frage wird durch die Richtlinie abschließend beantwortet: „Reverse Engineering" stellt keine Verletzung von Geschäftsgeheimnissen dar, solange keine abweichenden vertraglichen Regelungen getroffen wurden. Die einzige Möglichkeit für Unternehmen sich vor „Reverse Engineering" zu schützen, sind demnach Vertragsklauseln mit Zulieferern, Kunden und F&E-Partnern.

II. Einleitung

Jedes Unternehmen verfügt über eine Vielzahl von Informationen, deren wirtschaftlicher Wert darin besteht, dass sie Wettbewerbern nicht zur Verfügung stehen. Dabei kann es sich um geschäftsbezogene (z.B. Kundendaten, Strategien zur Geschäftsentwicklungen, Marktstudien, Zuliefererlisten) oder um technische Informationen (z.B. Konstruktionspläne, Herstellungsprozesse, Rezepturen) handeln.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0943&from=DE.

Informationen werden im Industrie-4.0-Zeitalter nicht länger auf Papier, sondern auf Servern gespeichert. Die Informationen einfach in einem Safe wegzuschließen, ist folglich kein probates Mittel zum Schutz von Geschäftsgeheimnissen mehr. Vielmehr bringt die Digitalisierung und Vernetzung von Arbeitsprozessen ein erhöhtes Risiko von Industriespionage und Geheimnisverrat mit sich. So zeigt eine Studie des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (Bitkom),[2] dass in den letzten zwei Jahren mehr als die Hälfte (53 Prozent) der deutschen Unternehmen Opfer von Industriespionage, Sabotage oder Datendiebstahls geworden sind. Der daraus entstehende Schaden wird auf 55 Milliarden Euro pro Jahr geschätzt. Die Risikofaktoren sind dabei vielfältig und können sowohl aus dem äußeren Unternehmensumfeld (z.B. durch konkurrierende Unternehmen, Hacker, Kunden und Lieferanten) als auch aus dem Unternehmen selbst (vor allem durch eigene Mitarbeiter) stammen. Der mit Abstand größte Risikofaktor für Geschäftsgeheimnisse sind nach der Bitkom-Studie ehemalige Mitarbeiter.

Die Studie zeigt, dass sich Unternehmen dauerhaft nur dann die Vorteile gegenüber Mitbewerbern bewahren können, wenn sie effektive Maßnahmen zum Schutz von Geschäftsgeheimnissen ergreifen. Der Geheimnisschutz ist damit mehr denn je wichtiger Faktor für den wirtschaftlichen Erfolg eines Unternehmens.

Dieses Whitepaper soll Unternehmen einen Überblick über die Rechtslage des Geheimnisschutzes auf europäischer Ebene und den Stand der Umsetzung in Deutschland und den Niederlanden verschaffen. Darüber hinaus soll es als Leitfaden für Unternehmen dienen, welche Geheimhaltungsmaßnahmen zu treffen sind, um den Schutz der Richtlinie in Anspruch nehmen zu können.

III. Hintergrund – die europäische Richtlinie zum Schutz von Geschäftsgeheimnissen

Ziel der Richtlinie (EU) 2016/943 ist im Wesentlichen die Harmonisierung des bisher fragmentarischen Schutzes von Geschäftsgeheimnissen in der Europäischen Union. Es soll ein einheitlicher Standard geschaffen werden, um vertrauliches Know-how und Geschäftsgeheimnisse vor Geheimnisverrat und Wirtschaftsspionage zu schützen und auf diese Weise grenzüberschreitende Innovationen im Binnenmarkt zu fördern.
Um als Geschäftsgeheimnis qualifiziert zu werden und den Schutz der Richtlinie in Anspruch nehmen zu können, muss eine Information geheim sein, aufgrund der Geheimhaltung einen kommerziellen Wert verkörpern und Gegenstand von angemessenen Geheimhaltungsmaßnahmen sein.

[2] https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf.

Erfüllt eine Information diese Voraussetzungen, ist sie vor (i) rechtswidrigem Erwerb, (ii) rechtswidriger Nutzung und rechtswidriger Offenlegung geschützt.

i. Der Erwerb eines Geschäftsgeheimnisses ist insbesondere dann rechtswidrig, wenn sich ohne Zustimmung des Inhabers unbefugter Zugang zur Information verschafft wurde oder sich die Information unbefugt angeeignet oder die Information unbefugt kopiert wird.

ii. Die Nutzung und Offenlegung ist rechtswidrig, wenn ein Geschäftsgeheimnis zuvor ohne Zustimmung des Inhabers rechtswidrig erworben wurde (siehe i.) oder gegen eine vertragliche Vereinbarung (z.B. Geheimhaltungsvereinbarungen, Wettbewerbsverbote) verstoßen wird.

Ein Unternehmen muss sich zudem den rechtswidrigen Erwerb, die Nutzung oder die Offenlegung eines Geschäftsgeheimnis zurechnen lassen, wenn das Geschäftsgeheimnis über einen Dritten erlangt wurde und man weiß oder wissen müsste, dass dieser das Geschäftsgeheimnis selbst unbefugt erlangt hat und deshalb nicht hätte nutzen oder offenlegen dürfen. Wird beispielsweise ein Mitarbeiter von einem Wettbewerber abgeworben und nutzt trotz eines vertraglichen Wettbewerbsverbots Geschäftsgeheimnisse seines ehemaligen Arbeitgebers auch bei seiner neuen Stelle, so dürfte auch der neue Arbeitgeber wegen Verletzung von Geschäftsgeheimnissen in Anspruch genommen werden, wenn für den neuen Arbeitgeber ersichtlich war, dass ein Wettbewerbsverbot bestand. Gerade bei Jobwechseln von höherrangigen Arbeitnehmern, die üblicherweise einem Wettbewerbsverbot unterliegen, ist es für den neuen Arbeitgeber deshalb unerlässlich im Arbeitsvertrag mit dem Arbeitnehmer durch Abwehrklauseln sicherzustellen, dass dieser die dem Wettbewerbsverbot unterliegenden Informationen des ehemaligen Arbeitgebers nicht bei seinem neuen Arbeitgeber einbringt.

Das sog. „Whistleblowing" soll dagegen keine rechtswidrige Offenlegung darstellen, wenn Geschäftsgeheimnisse an die Presse weitergegeben werden, die von öffentlichem Interesse sind. Auch „Reverse Engineering" soll ausdrücklich keine rechtswidrige Verletzung von Geschäftsgeheimnissen darstellen.

Um einen möglichst umfangreichen Schutz von Geschäftsgeheimnissen zu gewährleisten, stellt die Richtlinie dem Inhaber von Geschäftsgeheimnissen mehrere Ansprüche gegen den Verletzer zur Verfügung, die dieser nebeneinander geltend machen kann. So kann der Inhaber von Geschäftsgeheimnissen vom Verletzer

- Unterlassen der Nutzung oder Offenlegung des Geschäftsgeheimnisses,
- Schadensersatz,

- Vernichtung, die Beschlagnahme oder den Rückruf der das Geschäftsgeheimnis verletzenden Produkte vom Markt fordern, und/oder
- das Herstellen, Anbieten, Vermarkten, die Nutzung und die Aus- und Einfuhr das Geschäftsgeheimnis verletzender Produkte verbieten lassen.

Damit die Geschäftsgeheimnisse auch im Verlauf eines Gerichtsverfahrens geheim bleiben, sollen die Mitgliedstaaten sicherstellen, dass Informationen, die vom Gericht als geheimhaltungsbedürftig eingestuft wurden, nicht genutzt oder offengelegt werden. Deshalb sind alle am Verfahren beteiligten Personen (z.B. Richter, Anwälte, Zeugen, Sachverständige) auch über das Verfahren hinaus zur Geheimhaltung zu verpflichten. Des Weiteren sollen die Mitgliedstaaten sicherstellen, dass die Gerichte selbst spezifische Maßnahmen zur Geheimhaltung treffen können. Dies kann beispielsweise durch den Ausschluss der Öffentlichkeit, Zugangsbeschränkungen für geheime Informationen und das (teilweise) Nichtveröffentlichen gerichtlicher Entscheidungen geschehen.

Die Richtlinie war bis zum 8. Juni 2018 in nationales Recht umzusetzen. Deshalb können sich Einzelpersonen seit dem 9. Juni 2018 in gewissem Umfang unmittelbar auf die Richtlinie selbst berufen und verlangen, dass das nationale Recht richtlinienkonform auszulegen ist. Daher sind die Vorschriften der Richtlinie seit dem 9. Juni 2018 für alle in Europa tätigen Unternehmen unmittelbar relevant, unabhängig davon, ob die Richtlinie bereits in nationales Recht umgesetzt wurde oder nicht.

IV. Derzeitige Entwicklungen in Deutschland – Das Geschäftsgeheimnisgesetz

Am 18. Juli 2018 hat die Bundesregierung einen Entwurf eines eigenständigen Gesetzes zum Schutz von Geschäftsgeheimnissen beschlossen.[3] Der Bundesrat hat am 21. September 2018 zahlreiche Änderungen vorgeschlagen, weshalb das Gesetzgebungsverfahren derzeit stockt und ein Inkrafttreten nicht vor Mitte 2019 zu erwarten ist.
Besonders kontrovers diskutiert wird die Abgrenzung von Geschäftsgeheimnissen des Unternehmens auf der einen und erworbenen Fachkenntnissen und Berufserfahrungen von Arbeitnehmern auf der anderen Seite. Der derzeitige Entwurf könnte nach Meinung der Kritiker dazu führen, dass der Arbeitgeber das gesamte Know-how eines Arbeitnehmers als Geschäftsgeheimnis deklariert. Dies könne zur Folge haben, dass dem Arbeitnehmer ein Jobwechsel in der gleichen Branche erheblich erschwert oder gar unmöglich gemacht werde, weil er bei Anwendung seines erworbenen Know-hows beim neuen Arbeitgeber stets Gefahr liefe, Geschäftsgeheimnisse des vorherigen Arbeitgebers zu verletzen.

[3] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/GeschGehG.html.

Der Regierungsentwurf des Geschäftsgeheimnisschutzgesetztes orientiert sich ganz überwiegend an der zugrundeliegenden Richtlinie. Über die Anforderungen der Richtlinie hinaus sieht der Entwurf im Falle der Verletzung auch einen Auskunftsanspruch gegen den Verletzer vor, der sich auf

- Hersteller, Lieferanten, Abnehmer, Mengen und Kaufpreise der rechtsverletzenden Produkte,
- Dokumente, Gegenstände oder elektronische Dateien, die das Geschäftsgeheimnis enthalten oder verkörpern, und
- auf Personen, die das Geschäftsgeheimnis erlangt haben,

bezieht. Darüber hinaus drohen Personen, die Informationen nutzen oder offenlegen, die sie aufgrund eines gerichtlichen Prozesses erworben haben, Maßnahmen wie Ordnungsgeld und Ordnungshaft.

V. Derzeitige Entwicklungen in den Niederlanden – Wet bescherming bedrijfsgeheimen

In den Niederlanden wurde die Richtlinie bereits durch das Wet bescherming bedrijfsgeheimen in nationales Recht umgesetzt. Das Gesetz ist am 23. Oktober 2018 in Kraft getreten. Das Gesetz orientiert sich im Wesentlichen an dem Wortlaut der Richtlinie, sodass die vorgenannten Richtlinieninhalte in den Niederlanden unmittelbar gelten.
Über den Inhalt der Richtlinie hinausgehend sieht ein neuer Titel in der niederländischen Prozessordnung vor, dass – ähnlich wie bei Verletzungen geistiger Eigentumsrechte – auch bei Prozessen betreffend die Verletzung von Geschäftsgeheimnissen Beweismittel beschlagnahmt werden können. Darüber hinaus kann ein Verletzer von Geschäftsgeheimnissen dazu verurteilt werden, die im Prozess angefallenen Kosten des Inhabers des Geschäftsgeheimnisses zu tragen.

VI. Strategien für einen effektiven Schutz von Geschäftsgeheimnissen

In der europäischen Union tätige Unternehmen sollten die vorgenannten Auswirkungen der Richtlinie berücksichtigen und ihre Strategien für den effektiven Schutz von Geschäftsgeheimnissen neu bewerten. Die empfohlenen Geheimhaltungsmaßnahmen hängen von den spezifischen Umständen des Einzelfalles ab, wie z.B. dem Wert eines Geschäftsgeheimnisses für das Unternehmen und lassen sich in drei Bereiche unterteilen:

1. Organisatorische Maßnahmen

Zunächst sollten Unternehmen ein zentrales Know-how-Management-System etablieren, um Know-how und Geschäftsgeheimnisse sowie deren Träger zu identifizieren und zu kategorisieren. Insbesondere sollte sich jedes

Unternehmen über die eigenen „Kronjuwelen" – diejenigen Informationen, die für den Geschäftserfolg des Unternehmens besonders wichtig sind – gewahr werden. Mit Hilfe des Know-how-Management-Systems sollten die potentiellen Risiken für die Verletzung des jeweiligen Geschäftsgeheimnisses evaluiert und Abwehrmaßnahmen vorbereitet werden.

Zudem sollten anhand des Know-how-Management-Systems klare Verantwortlichkeiten und Zugangsrechte definiert werden. Je wichtiger die jeweilige Information für den Geschäftserfolg des Unternehmens ist, desto strikter sollten die Zugangsrechte gehandhabt werden. Besonders ratsam ist in diesem Zusammenhang die Einrichtung einer „need-to-know-Policy". Jeder Mitarbeiter sollte nur zu solchen Informationen Zugang haben, die er für seine Arbeit benötigt. Beispielsweise wird die Buchhaltung des Unternehmens für ihre Arbeit im Normalfall keinen Zugang zu detaillierten Informationen eines Herstellungsprozesses benötigen.

Als Teil des zentralen Know-how-Management-Systems sollte ein Notfallmanagement etabliert werden, um im Falle konkreter Gefährdungen für Geschäftsgeheimnisse von innen oder außen sofort reagieren zu können.

Darüber hinaus sollte ein wirksames Besucher-Management errichtet werden, um von vornherein auszuschließen, dass Besucher des Unternehmens mit Geschäftsgeheimnissen in Berührung kommen. Dies kann durch eine Identitätsfeststellung vor Einlass und die Verpflichtung zum Tragen eines Besucherausweises realisiert werden, welcher den Mitarbeitern ins Bewusstsein ruft, dass es sich nicht um einen Kollegen handelt. Auch kann ein Verbot von Smartphones mit Kameras ein wirksames Mittel darstellen.

Eines der größten Risiken für Geschäftsgeheimnisse eines Unternehmens ist häufig das mangelnde Bewusstsein der Mitarbeiter beim Umgang mit geschäftlichen Informationen. Deshalb ist es wichtig, eine Sicherheitskultur im Unternehmen zu etablieren und zu leben. Dies kann mit regelmäßigen Sicherheits-Trainings für die Mitarbeiter geschehen. Insbesondere sollten die Mitarbeiter im Umgang mit privaten und geschäftlichen mobilen Endgeräten und Speichermedien geschult werden. In den meisten Fällen empfiehlt es sich sogar, private Speichermedien vollständig zu verbieten. Auch die unreflektierte Nutzung von bestimmten Apps, Programmen und Webseiten kann zum Verlust von geheimen Informationen führen. Darüber hinaus sollten den Arbeitnehmern klare Richtlinien beim Umgang mit Geschäftsgeheimnissen vorgegeben werden. Inhalt solcher Richtlinien kann beispielsweise die Verpflichtung sein, den Computer am Arbeitsplatz bei Abwesenheit zu sperren

sowie das Verbot Unterlagen mitzunehmen oder fremde Software auf Dienstgeräten zu installieren.

Es ist darüber hinaus empfehlenswert zu evaluieren, ob Geschäftsgeheimnisse durch technische Schutzrechte wie Patente oder Gebrauchsmuster geschützt werden können. Besonders bei Produkten oder Herstellungsprozessen bietet sich diese Schutzmöglichkeit an.

Alle ergriffenen Maßnahmen und weitergegebene Informationen – etwa an Zulieferer, Kunden oder F&E-Partner – sollten unbedingt dokumentiert werden. Eine lückenlose Dokumentation ist für Geheimnisverletzungsprozesse unabdingbar, weil jedes Unternehmen die getroffenen „angemessenen Maßnahmen" nachweisen muss. Im schlimmsten Fall kann eine unvollständige Dokumentation zum Verlust aller Ansprüche aus der Verletzung von Geschäftsgeheimnissen führen.

2. Rechtliche Maßnahmen

Unternehmen sollten zudem vertragliche Maßnahmen ergreifen, um ihre Geheimhaltungsinteressen zu wahren. Dies betrifft zum einen Arbeitsverträge mit Mitarbeitern. Besondere Aufmerksamkeit sollte der Formulierung von Geheimhaltungsklauseln zuteil werden. Die Klauseln sollten detaillierte Regelungen und Richtlinien für den Umgang mit Know-how enthalten, um die Mitarbeiter von Anfang an für den Umgang mit geschäftlichen Geheimnissen zu sensibilisieren. Zudem sollten die Klauseln ausreichend detailliert und differenziert sein, um deren Wirksamkeit zu gewährleisten. Klauseln, die den Mitarbeiter pauschal zur Geheimhaltung aller geschäftlichen Belange verpflichten (sog. „catch-all-Klauseln"), sind nach der Rechtsprechung in Deutschland unwirksam. Mit Schlüsselarbeitnehmern sollte zudem ein nachvertragliches Wettbewerbsverbot mit einer Vertragsstrafe im Falle des Verstoßes vereinbart werden. Auch hier ist eine detaillierte und präzise Formulierung unabdingbar, denn die deutsche Rechtsprechung erkennt nachvertragliche Wettbewerbsverbote nur dann als wirksam an, wenn diese die weitere Karriere des Mitarbeiters nicht wesentlichen erschweren oder behindern.

Zum anderen betrifft dies Verträge mit Zulieferern, Kunden, Lizenznehmern und anderen Kooperationspartnern. Diese sollten für den Fall, dass geheime Informationen ausgetauscht werden, eine Geheimhaltungsvereinbarung enthalten. Auch „Reverse Engineering" lässt sich durch eine solche Geheimhaltungsvereinbarung ausschließen, die in der Praxis meist mit Vertragsstrafen und/oder Kündigungsrechten verbunden wird. Die

Formulierung solcher Geheimhaltungsvereinbarungen ist vor dem Hintergrund der detaillierten Rechtsprechung in Deutschland nicht unproblematisch und endet schnell in der Unwirksamkeit der Klausel. Es kann daher ratsam sein, rechtliche Beratung bei dem Entwurf solcher Klauseln in Anspruch zu nehmen.

3. Technische Maßnahmen

Die Strategien für den effektiven Schutz von Geschäftsgeheimnissen werden durch technische Maßnahmen komplettiert. Ein wirksames IT-System zum Schutz geheimhaltungsbedürftiger Informationen dürfte in jedem Unternehmen unabdingbar sein. Dies beinhaltet Firewalls und Verschlüsselungssysteme gegen Hackerangriffe sowohl auf dem internen System des Unternehmens als auch auf dienstlich genutzten Endgeräten. Zugangsautorisierungen für bestimmte betriebliche Geheimnisse sollen dauerhaft überwacht und regelmäßig auf den neuesten Stand gebracht werden. Besonders bei Ausscheidens eines Mitarbeiters aus dem Unternehmen sollte sichergestellt sein, dass keine Zugriffsmöglichkeiten auf die geheimen Informationen des Unternehmens mehr bestehen.

Zudem sollte bei der Übertragung und dem Abruf von geheimen Informationen technische Maßnahmen wie Passwortschutz und Verschlüsselungssysteme berücksichtigt werden. Die Passwörter sollten nicht zu einfach sein, um Hackern den Zugriff so schwer wie möglich zu machen. Zudem empfiehlt sich bei besonders wichtigen Informationen ein „2-Faktor-Authentifizierungssystem".

Die vorgenannten Maßnahmen sollten idealerweise durch Maßnahmen gegen physischen Datendiebstahl, wie etwa Videoüberwachungsanlagen und Eingangskontrollen, ergänzt werden.