Markus von Fuchs, LL.M.

„Praktische Konsequenzen der EU-Trade-Secrets-Directive für das Verhalten von Unternehmen“

Um weiterhin in den Genuss des gesetzlichen Schutzes von Geschäfts- und Betriebsgeheimnissen zu kommen, verlangt die EU Richtlinie von den Geschäftsinhabern „den Umständen entsprechende angemessene Geheimhaltungsmaßnahmen“. Was bedeutet dies in der Praxis für Unternehmen und welche konkreten Maßnahmen müssen ergriffen werden?

Im Juni 2016 wurde die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen, kurz Know-how Schutz Richtlinie verabschiedet. Nun rückt der 9. Juni 2018 näher, zu dem spätestens die Regelungen durch die Mitgliedsstaaten in nationales Recht umgesetzt sein müssen. Zwar steht noch nicht genau fest, wann die Umsetzung in Deutschland erfolgt, es wird jedoch für Unternehmen insbesondere dann höchste Zeit, sich mit den Auswirkungen auseinanderzusetzen, wenn deren Geschäftserfolg entscheidend von Know-how abhängt.

Betrachtet man nämlich genauer, was eigentlich mit Know-how gemeint ist, welches unter den Geltungsbereich der Richtlinie fällt, so wird einem zwangsläufig die volkswirtschaftliche Bedeutung der Richtlinie bewusst. Gemeint sind nämlich sowohl betriebliche Informationen, wie Businesspläne, Kundenlisten und Preisinformationen als auch Informationen technischer Natur, zu denen Pläne, technische Zeichnungen und sonstige technologische Informationen zählen.

Vor allem aber gehören auch Daten dazu.

Daten sind der Kern der technologischen und industriellen Revolution, die derzeit in sämtlichen industriellen und gesellschaftlichen Bereichen geschieht. Daten sind für viele Unternehmen zunehmend das hauptsächliche Vermögensgut und stellen die Infrastruktur und das Rückgrat der Digitalisierung dar. Das Problem ist aber, dass mangels entsprechender Regelungen, Daten nicht dem zivilrechtlichen Eigentumsbegriff und auch nicht dem geistigen Eigentum unterfallen und somit keinen Sonderrechtsschutz genießen.

Ein wirksamer Schutz von Daten ist derzeit nur über den Schutz von Geschäfts- und Betriebsgeheimnissen aus den §§ 17, 18 und 19 UWG möglich. Gerade hier aber setzt die Know-how Schutz Richtlinie an und verändert an einigen Stellen entscheidend die Pflichten der Inhaber solcher Geschäfts- und Betriebsgeheimnisse.

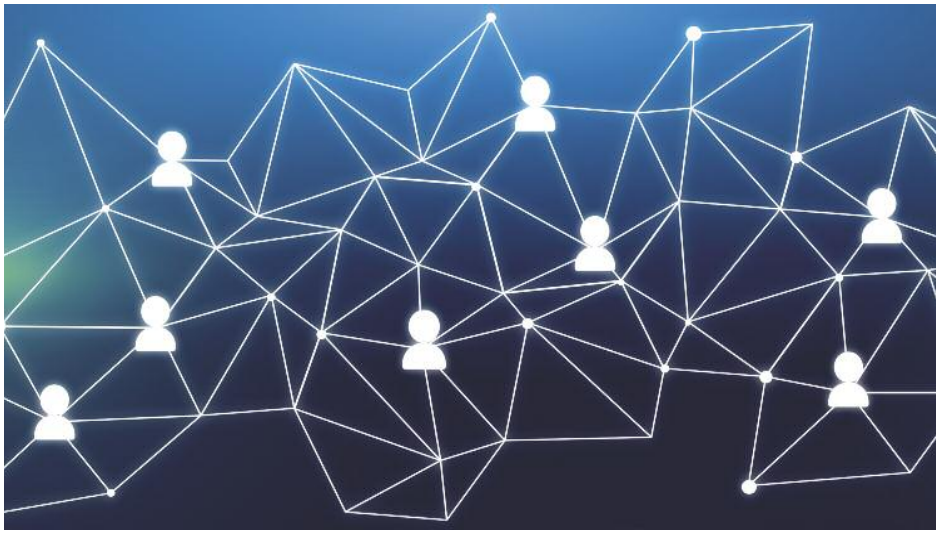
Fallen Daten unter den Begriff des Geschäftsgeheimnisses?

Das Problem ist häufig, dass einzelne Daten relativ leicht zugänglich sind und das Datum für sich genommen häufig keine geheime Information darstellt. Der Wert der Daten liegt aber vor allem darin, dass eine Vielzahl von Daten in einer bestimmten Form generiert und zusammengestellt ist, wodurch sie kommerziell nutzbar werden.

Eine exakte Definition, welcher Natur Informationen sein müssen, um ein Geschäftsgeheimnis sein zu können, erfolgt in der Richtlinie nicht. In Randnummer 14 der Erwägungen wird hierzu ausgeführt, dass eine Definition nicht dazu dienen soll, „den vor widerrechtlicher

Aneignung zu schützenden Bereich einzuengen“. Sie soll also weit gefasst sein und „Know-how, Geschäftsinformationen und technologische Informationen“ abdecken.

Interessant ist also nach der oben gemachten Vorbemerkung beispielsweise, wie die Richtlinie sich auf den Schutz von Daten auswirkt. Das einzelne Datum wird sicherlich dann nicht als Geschäftsgeheimnis anzusehen sein, wenn es sich um eine Information handelt, die frei erhältlich ist. Allerdings formuliert die Richtlinie in Art 2 Nr. 1 a): „...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“. Nun ergibt sich der Wert von Daten in der Regel aber aus einer Vielzahl an Informationen bzw. Daten und ihrer (sinnvollen) Kombination sowie deren Nutzbarkeit für kommerzielle Zwecke.



Genau hier aber verdeutlicht die Richtlinie, dass selbst wenn also Daten aus einer Vielzahl von an sich zugänglichen oder bekannten Informationen bestehen, sie dennoch als Geschäftsgeheimnis qualifizierbar sind, wenn ihre konkrete Zusammensetzung unbekannt ist.

Geheimhaltungspflicht

Eine große Änderung wird es bei der Pflicht des Geschäftsinhabers geben, sein betriebliches Know-how zu schützen. Geschäftsgeheimnis konnte bisher nur etwas sein, für das es auch einen Geheimhaltungswillen des Geschäftsinhabers gibt. In der Regel wurde dieser Geheimhaltungswillen durch die deutschen Gerichte vermutet, es sei denn, es ergaben sich Umstände, die an einem solchen Willen Zweifel aufkommen ließen. Hier setzt die Richtlinie an, die entgegen der bisherigen deutschen Rechtslage , nunmehr *„reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret“* also den Umständen entsprechenden angemessenen und dauerhafte Geheimhaltungsmaßnahmen verlangt, damit die Informationen überhaupt als Betriebs- oder Geschäftsgeheimnis anerkannt werden und in den Schutz der Vorschrift gelangen.

Welche Pflichten ergeben sich daraus für den Unternehmer?

Anders als bisher wird also der Unternehmer, der sich gegen einen Wettbewerber oder früheren Mitarbeiter wegen der Entwendung von Daten oder deren Verwendung wendet, darlegen und beweisen müssen, dass er dauerhafte Maßnahmen zum Schutz dieser Daten getroffen hat. Hiermit sind mitnichten nur juristische Vertragsklauseln gemeint, sondern ein umfangreiches System zum Know-how Schutz, welches ein Zusammenspiel von u.a. organisatorischen, technologischen, vertraglichen und personalbezogenen Maßnahmen erfordert. Berücksichtigt man beispielsweise die Tatsache, dass der überwiegende Teil der Entwendung von betrieblichem Know-how durch eigene Mitarbeiter erfolgt und dahinter häufig Unkenntnis der Rechtslage steckt, liegt hier sicherlich ein Schwerpunkt der erforderlichen Maßnahmen. So sollten entsprechende Klauseln in Arbeitsverträgen sowie regelmäßige Schulungen von Mitarbeitern, in denen diese für das Thema sensibilisiert werden, eigentlich Standard sein. Daneben sind insbesondere in sensiblen Bereichen auch organisatorische Vorkehrungen, wie z.B. das strikte Einführen eines „Need-to-know“ Prinzips ein probates Mittel. Nicht jeder Mitarbeiter muss alles wissen und auf alle Daten Zugriff haben, wenn er dies nicht zur Erfüllung seiner Arbeit benötigt. Auch reichlich stiefmütterlich werden in deutschen Unternehmen nach wie vor technologische Maßnahmen zum Schutz vor externem und internem Zugriff getroffen, obwohl diese sowohl tatsächlich geeignet sind, geheime Informationen zu sichern, als auch in Zukunft entscheidend dafür sind, ob Informationen als Geschäftsgeheimnis anzusehen sind.

In Zukunft wird man als Unternehmen nachweisen müssen, dass man hier ausreichende und angemessene Vorkehrungen getroffen hat, sein Know-how zu schützen. Gelingt dies nicht, wird eine erfolgreiche Durchsetzung seiner Ansprüche nicht mehr möglich sein.

Bewertung von Geschäftsgeheimnissen

Der Inhaber wird zukünftig auch nachweisen müssen, dass das zu schützende Geschäftsgeheimnis einen bestimmten Wert hat. Nach bisheriger Rechtslage war dies nicht erforderlich. Nach der Rechtsprechung reichte es aus, dass der Inhaber ein berechtigtes Interesse daran hat, dass sein Wettbewerber keine Kenntnis von den Informationen hat, insbesondere wenn sich dies nachteilig auswirken könne. Dies wird so vermutlich in Zukunft nicht mehr ausreichen. Denn in Art. 2 Nr. 1 b) der Richtlinie wird gefordert, dass den Informationen ein kommerzieller Wert zukommen soll, dadurch dass sie geheim sind. Was damit gemeint ist, erklärt sich aus den Erwägungsgründen der Richtlinie in denen unter Randnummer 14 erklärt wird, dass den Informationen ein realer oder potentieller Handelswert zukommen müsse. Dem Inhaber muss bei Entwendung also ein wirtschaftlicher Schaden entstehen, dadurch dass er nicht mehr alleinige Verfügungsmacht darüber hat. Von einigen Kommentatoren wird hiermit bereits die Auffassung vertreten, wonach Know-how bilanziert werden müsse, um überhaupt dem Schutz des Gesetzes zu unterfallen. Selbst wenn man so weit nicht gehen möchte, so wird zukünftig wohl vom Inhaber gefordert werden, das Know-how mit nachvollziehbaren Kriterien zu bewerten.

Reverse Engineering grundsätzlich erlaubt

Die Richtlinie macht insbesondere in Randnummer 16 seiner Erwägungen deutlich, dass die Bestimmungen zum Schutz von Geschäftsgeheimnissen keinen Sonderrechtsschutz an betrieblichem Know-how begründet. Wer rechtmäßig in Besitz solchen Know-hows gelangt, soll auch nicht daran gehindert sein, dieses zu nutzen. So soll es auch im Wege des sog. Reverse-Engineerings erlaubt sein, erworbene Geräte, in denen sich betriebliches Know-how manifestiert, auseinanderzubauen, um an die Informationen zu gelangen. Hier bleibt nur eine vertragliche Vereinbarung, welche es dem Kunden untersagt, solcherart an Informationen zu kommen und sie für sich zu nutzen.

Zusammenfassung

Unternehmen werden sich zukünftig proaktiv damit befassen und entscheiden müssen, ob und mit welcher Intensität sie sich um den Schutz ihres betrieblichen Know-hows kümmern. Da es sich hierbei oft um die wichtigsten Assets eines Unternehmens handelt, wird es vor allem für das Management keine Ausreden für den Fall mehr geben, dass solches Know-how abhanden kommt. Der Schutz von Know-how muss also gerade für innovative Unternehmen als eine zentrale Aufgabe des Managements begriffen werden. ◀