LIEB. RECHTSANWÄLTE

Know How – Richtlinie
Geheimnisschutz aus Europa – Handlungsbedarf im Unternehmen

LIEB.Rechtsanwälte, Erlangen / Nürnberg

Stand: 03/2019

Inhalt

I. Einleitung

Europa wappnet sich nun endlich auch im juristischen Bereich für ein (neues) Technikzeitalter. Bislang sind die meisten nationalen Rechtsordnungen, die alle im Grunde auf jahrhundertalte Normkomplexe zurückgehen, nicht oder nur unzureichend auf die Gegebenheiten der aktuellen Technik angepasst. Daher besteht nunmehr dringender Handlungsbedarf.

Know How ist der Motor vieler innovativer Unternehmen. Hier zeigt sich ein besonders sensibler Bereich für die Wirtschaft für morgen. Bereits bestehender technischer Vorsprung zu anderen Mitbewerbern muss genauso geschützt werden wie neue bahnbrechende Innovationen. Im Zeitalter der Postindustrialisierung gilt das für jeden: vom *start up entrepreneur* bis hin zum milliardenschweren Konzern. Die Bedrohung durch Wirtschaftsspionage und Geheimnisverrat dürfte mit der zu erwartenden weiteren Technisierung weiter zunehmen. Um dieser Gefahrenlage effizient begegnen zu können, bedarf es einem Zusammenspiel aus Gesetzgebung und unternehmensinterner Präventionsmaßnahmen.

Diese Wichtigkeit hat nunmehr auch der europäische Gesetzgeber erkannt und versucht den Schutz zu stärken sowie europaweit zu vereinheitlichen. Wer sich allerdings hierauf berufen will, muss auch die entsprechenden Voraussetzungen erfüllen.

Unser Leitfaden soll Ihnen einen Überblick über relevante Fragestellungen geben. Unser Team steht Ihnen ferner jederzeit zur juristischen Lösung Ihrer Frage- und Problemstellungen zur Verfügung.

II. Impulse aus Europa

1. *Know How*-Richtlinie kompakt

Heimlich, still und leise und von vielen unbemerkt schlich sich die *Know How*-Richtlinie der Europäischen Union (Richtlinie (EU) 2016/943, vom 8. Juni 2016) auf das Radar geltender deutscher Rechtsnormen.

Grundsätzlich stellen Richtlinien der EU zwar nur Weisungen an die Mitgliedsstaaten dar, dass die in der Richtlinie getroffenen Bestimmungen bis zu einer bestimmten Frist verbindlich in nationale Gesetze umzuwandeln sind (Art. 288 Abs. 3 AEUV). Sollte der Staat eine solche Frist allerdings versäumen, wird dies europarechtlich dadurch sanktioniert, dass ab diesem Zeitpunkt nunmehr unmittelbar der Richtlinientext verbindlich gilt. Damit können sich nahezu unbemerkt Rechtsänderungen mit weitreichenden Folgen ergeben. Höchste Vorsicht ist dann geboten, wenn sich ein solcher Wandel in Kerninhalten, wie etwa dem Geheimnisschutz, vollzieht.

Genau dies ist jedoch hier passiert. Der deutsche Gesetzgeber hat die Richtlinie der EU nicht fristgerecht zum 9. Juni 2018 umgesetzt. Seither gilt diese – von vielen weitgehend unbemerkt – unmittelbar. Wer böse Überraschungen vermeiden will, sollte nun auch unternehmensintern handeln.

Ein Entwurf aus Berlin für ein nationales Umsetzungsgesetz, mit der Bezeichnung Geschäftsgeheimnisgesetzes und der weniger wohlklingenden Abkürzung *GeschGehG*, ist nunmehr aber auf den Weg gebracht. Der Gesetzesentwurf ist auf der Website des BJVM abrufbar.

Wir informieren Sie hier kurz und knapp über die wesentlichen Inhalte, die bald auch durch nationale Gesetze verankert sein dürften.

2. Europas neuer Geheimnisbegriff

Europa hat ein anderes Verständnis für den Begriff des Geschäftsgeheimnisses. Waren dies nach deutschem Verständnis bislang

„*alle im Zusammenhang mit einem Betrieb stehenden Tatsachen, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt sind und nach dem bekundeten Willen des Betriebsinhabers, der auf einem ausreichenden wirtschaftlichen Interesse beruht, geheim gehalten werden sollen*“,

liegt dies nunmehr ein klein wenig anders.

Aus Europa kommt nun im Wesentlichen eine weitere Voraussetzung hinzu. Geschäftsgeheimnisse sind nach Art. 4 Nr. 1 der Richtlinie nunmehr Informationen, die:

- geheim sind, in dem Sinne, 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;

- sie aus diesem Grund von kommerziellem Wert sind

und – und eben genau diese Voraussetzung ist neu -

- *Gegenstände von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch den rechtmäßigen Inhaber sind.*

Soweit so klar? Leider nein.

Zwar lässt sich dem Art. 4 Nr. 1 c) entnehmen, dass nunmehr angemessene Geheimhaltungsmaßnahmen notwendig sind. Allerdings hält sich die Richtlinie in der Bestimmung dieser Angemessenheit sehr zurück. Auch der Gesetzesentwurf aus Berlin ist hier eher dürftig. Dort findet sich die Begriffsdefinition in § 2 Nr. 1 *GeschGehG (E)*. Derzeit bekannt ist nur, dass hierunter sowohl physische und technische Vorkehrungen sowie vertragliche Sicherungskonzeptionen fallen können.

Nach der Entwurfserläuterung zum deutschen Umsetzungsgesetz sei es nicht erforderlich, jede geheim zu haltende Information gesondert zu kennzeichnen. Es sei ausreichend, wenn für bestimmte Kategorien von Informationen Maßnahmen, etwa technische Zugangshürden, oder allgemeine interne Richtlinien und Anweisungen ergriffen würden. Ferner könne der entsprechende Schutz durch Anpassungen im Arbeitsvertrag hergestellt werden.

Insbesondere die Angemessenheit wird aber in Zukunft wohl sowohl den Unternehmer als auch die Gerichte beschäftigen. Der Gesetzgeber hat es sich relativ einfach gemacht. Die Angemessenheit sei nach dem Einzelfall zu bestimmen. Hierbei können aber insbesondere - und damit nicht abschließend – folgende Kriterien erheblich sein:

- der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten,
- die Natur der Informationen,
- deren Bedeutung für das Unternehmen,
- die Größe des Unternehmens,
- die Art der Informationskennzeichnung
- die getroffenen vertraglichen Regelungenmit Arbeitnehmern und Geschäftspartnern.

Übrigens sollten sich nicht nur Unternehmer Gedanken über die *Know How*-Richtlinie machen. Auch Lizenznehmer kann die Pflicht zu angemessenen Geheimhaltungsmaßnahmen treffen.

3. Reverse Engineering

Mit Reverse Engineering bezeichnet man einen Vorgang, in dem ein marktfertiges und für die Allgemeinheit erwerbliches Produkt analysiert und zur Extraktion fremder, meist technischer Erkenntnisse rückgebaut wird.

Das Reverse Engineering war bisher rechtlich nicht ganz eindeutig geklärt. Nachbauten, die gegen Patentrechte verstießen, waren und sind auch zukünftig unzulässig und dementsprechend sanktionierbar. Bei nicht-patentierten Produkten war die Lage deutlich schwieriger zu beurteilen. Hier blieb oft nicht viel mehr als der wettbewerbsrechtliche Nachahmungsschutz.

Im Bereich des Reverse Engineering bildet sich nunmehr aber ein Paradigmenwechsel ab. Nach deutschem Verständnis galt das Reverse Engineering bislang im Wesentlichen als unzulässig. Art. 3 lit. b) der Geheimnisschutzrichtlinie erlaubt nunmehr grundsätzlich das Reverse Engineering. Inhalt des Reverse Engineering ist die Analyse von erfolgreichen Produkten. Hierbei werden insbesondere Konstruktionen und technische Funktionsweise mit dem Ziel eines Nachbaus und einer Parallelvermarktung untersucht.

Hardware Reverse Engineering ist hierbei die klassische Variante, die so letztlich schon seit der industriellen Revolution betrieben wird. Vorreiter dieser Industriespionage waren anfangs vor allem das Militär und Geheimdienste, später kam es auch in der freien Wirtschaft an und stellt für Unternehmen eine deutliche Gefährdungslage dar. In Zeiten der Technologisierung spielt das Reverse Engineering aber auch im Softwarebereich eine zunehmende Rolle. In diesem Zusammenhang sind vor allem die Quellcodes von Softwares und Apps von besonderer Schutzbedürftigkeit, um einer Programmkopie entgegen zu wirken.

Wie Sie Ihr Unternehmen gegen diese Bedrohungslage wappnen können, finden Sie in der Rubrik „Handlungsbedarf“.

4. Geheimnisschutz im Prozess

Um die Geheimhaltung muss sich jedenfalls im Prozess nicht mehr allein der Unternehmer kümmern. Sowohl in der Richtlinie als auch im deutschen Entwurf für das Umsetzungsgesetz finden sich Regelungen wie die Geheimhaltung auch im Gerichtsverfahren zu gewährleistein ist. Hier gibt es die Möglichkeit streitgegenständliche Informationen durch das Gericht als geheimhaltungsbedürftig einstufen zu lassen. Dem Gericht verbleibt hier aber ein gewisses Ermessen, wann solche vorliegen. Alle Prozessbeteiligten sind dann verpflichtet dass vertrauliche Informationen, die im Verfahren erlangt wurden, nicht nach außen offengelegt oder genutzt werden. Bei Zuwiderhandlung drohen empfindliche Ordnungsgelder oder gar Ordnungshaft. Die Pflicht der Geheimhaltung gilt dann auch für die Zeit nach Abschluss des Verfahrens. Zum Geheimnisschutz kann auch die Öffentlichkeit aus dem Gerichtssaal ausgeschlossen werden. Dies ist aus Unternehmersicht zwar das Mindeste. In der deutschen Rechtsordnung, in der grundsätzlich aber der Öffentlichkeitsgrundsatz für Pro-

zesse gilt, ist dies aber durchaus eine Besonderheit. Dass der Geheimhaltungsaspekt auch im Prozess unabdingbar ist, hat auch der deutsche Gesetzgeber in seinem Entwurf bedacht und Regelungen hierzu in Abschnitt 3 des Entwurfsgesetzes aufgenommen. Aufgrund der Unsicherheiten der praktischen Umsetzung des Geheimnisschutzes im Prozess ist die Vereinbarung einer Schiedsgerichtsbarkeit mit wichtigen Vertragspartnern weiterhin eine attraktive Alternative.

III. Handlungsbedarf im Unternehmen

1. Vertragliche Geheimhaltungsmaßnahmen

Wo Geschäftsgeheimnisse und Kommunikationsvorgänge zusammentreffen sollte künftig besonderer Wert auf vertragliche Geheimhaltungsmaßnahmen gelegt werden. Mit der neuen *Know How*-Richtlinie sind nunmehr die oben bereits erwähnten angemessenen Geheimhaltungsmaßnahmen notwendig.

Das Spannungsfeld in diesem Kontext ist komplex. Dürfen die *Non disclosure agreements* (NDAs) einerseits nicht zu strikt sein, damit man die künftigen Vertragspartner nicht verschreckt, müssen sie andererseits den Schutz ausreichend gewährleisten. Hier sollte man einen verlässlichen Partner und Berater aufsuchen. Die Rechtslage ist vor allem in Bezug auf die neue Richtlinie noch relativ unklar. Nur wer aktuelle Entwicklungen verfolgt, kann entsprechend agieren.

NDAs als solches sind kein Novum. Sie bilden bereits heute vielfach Bestandteil von Verträgen, Erfahrungen aus der bisherigen Judikatur können hierbei also jedenfalls Orientierungshilfe bilden.

Sowohl in der Richtlinie, als auch im Gesetzesentwurf sowie in einigen bereits bestehenden Gesetzen finden sich Bestimmungen über Rückgabe oder Vernichtung verkörperter Informationen, wenn das Vertragsverhältnis endet. Das schließt jedoch nicht aus, dies nochmals und auf den konkreten Einzelfall angepasst in die *NDAs* aufzunehmen.

Nicht nur für die Zukunft ist Handlungsbedarf zu sehen. Auch die Evaluierung und Bewertung der aktuellen Lage kann sinnvoll oder bisweilen gar notwendig

sein. Man denke an befristete Verträge, die kurz vor einer Verlängerungen stehen. Diese sollten daraufhin überprüft werden, ob sie mit den aktuellen Anforderungen im Gleichklang stehen. Aber bei auch bestehenden unbefristete Verträge sollte eine Bewertung stattfinden.

Zu beachten ist ferner, dass die Verschwiegenheit auch über das Vertragsverhältnis vereinbart werden sollte. Hierzu sollten Rückgabe- und Löschungspflichten für sämtliche im Zusammenhang mit der Betätigung erlangten Dokumente und Daten vereinbart werden. Aber eben auch die Nutzungsuntersagung oder Verbreitung der Geheimnisse an Dritte.

a) Vertragliche Bestimmung von Geheimnissen

Grundsätzlich empfiehlt es sich immer, den Schutzgegenstand klar zu bestimmen und zu bestimmen wo die Grenzen zwischen erlaubter und untersagter Nutzung liegen. Die Meinungen wie spezifisch man vorgehen muss, divergieren hierbei deutlich. Die einen fordern eine stringente Auflistung aller Geschäftsgeheimnisse und Qualifikation dieser Informationen als eben solche. In der Praxis hingegen stößt man oft auf sehr allgemein gehaltene Formulierungen. Diese sprechen dabei oft von „alle Geschäftsgeheimnisse“.

Eine allgemeine Verschwiegenheitsklausel sollte aus Sicherheitsgründen wohl in jedem Vertrag zu finden sein. Bei Geheimnisträgern, also jenen, die wirklich mit den wesentlichen Informationen der Geschäftsgeheimnisse – etwa den konkreten Mischverhältnissen einer Rezeptur - in Kontakt kommen, kann eine konkretere Aufzählung empfehlenswert sein. Dabei sollte man stets mit einer *insbesondere*-Aufzählung arbeiten. Der Vorteil hierin besteht darin, dass die aufgezählten Geheimnisse rechtstechnisch nicht abschließend sind. So wird etwa dem Mitarbeiter oder Vertragspartner deutlich was konkret unter Geheimnis in diesem Sinne zu verstehen ist. Andererseits wird der technische Fortschritt damit vertraglich schon mit eingearbeitet. Auch zukünftig entwickelte Geheimnisse könnten dann mit umfasst werden, ohne dass kontinuierlich eine zeit- und kostenaufwendige Anpassung des Vertrags notwendig würde.

b) Vertragsstrafen

Zum Schutz der Geheimnisse können in Verträge Vertragsstrafen aufgenommen werden. Im Falle von NDAs ist jedoch Zurückhaltung geboten, da in der Praxis regelmäßig gegenseitige NDAs abgeschlossen worden. Eine Vertragsstrafe kann so schnell zum Boomerang werden. Der Vorteil einer Vertragsstrafe liegt klar darin, dass keine konkrete Schadenshöhe durch den Unternehmer bewiesen werden muss.

Auch bei der Höhe sind Grenzen zu beachten. Grundsätzlich gilt, dass die verletzte Geheimhaltungspflicht den Maßstab für die Höhe der Verstragstrafe bildet. In diesem Zusammenhang spielt auch das vereinbarte Entgelt eine wichtige Rolle. Aus diesen beiden Aspekten ist dann zu bestimmen wo die Grenze zwischen einer wirksamen und einer unwirksamen Vertragsstrafklausel liegt.

c) Reverse Engineering-Klausel

Das Reverse Engineering ist Grundlage eines Risikos, das die Richtlinie mit sich gebracht hat. Wer sich davor schützen möchte, dass Vertragspartner hiervon Gebrauch machen, muss sich vertraglich absichern. Dies kann über eine Reverse Engineering-Verbotsklausel erreicht werden. Die Geschäftspartner verpflichten sich, etablierte Produkte des anderen nicht rückzubauen, um so einem Nachbau und der Parallelvermarktung vertraglich vorzubeugen. Damit das Verbot auch wirkungsvoll ist, wird dieses dann auch mit einer Vertragsstrafe verbunden. Sollte ein Rückbau erfolgen, muss später nur dieser nachgewiesen werden, nicht hingegen ein konkreter Schaden und vor allem dieser nicht beziffert werden.

2. Organisatorische und technische Geheimhaltungsmaßnahmen

Der Geheimnisschutz lässt sich auch über Maßnahmen bewerkstelligen, die ursprünglich aus dem Datenschutz und der IT-Sicherheit stammen.

Ein Bedrohungspotential für geheime Informationen besteht nicht nur dort wo Menschen miteinander kommunizieren. Auch dort wo technische Mittel zum Einsatz kommen, sollte man Vorsicht walten lassen. Insbesondere wenn die Technik über Unternehmensnetzwerke von verschiedenen Endgeräten genutzt werden kann und umso mehr dort wo auch noch ein Zugang zum Internet besteht.

Technische Maßnahmen umfassen insofern vor allem eine sichere Netzwerkarchitektur. Der Schutz von unbefugten Zugriffen ist dabei immens wichtig. Hierbei ist der aktuelle Stand der Technik zu beachten. Zum einen ist es möglich, die Zugriffsberechtigungen abzustufen. Nicht jeder Ihrer Mitarbeiter benötigt einen Vollzugang zu allen Unternehmensdaten. Daher sollte der Zugriff auch stets nur soweit gehen, wie es zur Erfüllung der Aufgaben auch erforderlich ist.

Weiterhin gibt es die Möglichkeit Zugriffe zu dokumentieren. Hierbei muss man freilich abwägen, wo der Geheimnisschutz die Dokumentierung rechtfertigt und wo eine solche zu weit geht.

Auch Schulungen oder Informationsmaterial im Umgang mit Geheimnissen für die Mitarbeiter können und sollten implementiert werden. Diese Compliance-Maßnahmen können dabei vielfältig ausfallen. Ein Kurzleitfaden der schnellen Zugriff gewährt, sollte jedem Ihrer Mitarbeiter zugänglich sein. Das informiert und gibt dem einzelnen Mitarbeiter eine gewisse Sicherheit. Für Angestellte in Positionen, in denen ein Umgang mit Geheimnissen alltäglich oder jedenfalls keine Seltenheit ist, könnten regelmäßig Unterrichtseinheiten angeboten oder sogar angeordnet werden. Der Unterricht kann dabei nicht nur durch einen persönlichen Vortrag gestaltet werden, sondern auch modern und softwareunterstützt. Sollte jedoch einmal Unklarheit bestehen, muss den Mitarbeitern bekannt sein, wohin sie sich wenden können. In kleineren Unternehmen wird das meist die Geschäftsführung sein. Sollte in Ihrem Unternehmen aber bereits eine Compliance-Abteilung eingerichtet sein, könnte man auch dort eine Kontaktperson dafür benennen.

Überragend wichtig, um in den Genuss des Geheimnisschutzes zu kommen, ist eine fundierte Dokumentation welche Maßnahmen vom Unternehmer unternommen wurden. Künftig wird eben dieser nämlich die Beweislast tragen müssen, ob die Voraussetzungen an en Geheimnis erfüllt sind. Wer kein System der Dokumentation der Schutzmechanismen etabliert hat, steht dann vor Gericht

mit leeren Händen. Diese Situation gilt es dringend zu vermeiden. Welche Maßnahmen sich für Sie anbieten oder gar notwendig erscheinen, entscheiden Sie natürlich selbst. In jedem Fall sollte man zunächst Inventarisieren, welche Informationen im Unternehmenswissen befindlich sind und diese anschließend nach Wertigkeit und Wichtigkeit kategorisieren. Hierbei sind möglichst umfassend potentielle Risikolagen aufzudecken. Im darauffolgenden Schritt sollte man Zusammen mit einem Expertenteam des Vertrauens ein Konzept erarbeiten. Dabei empfiehlt es sich verschiedene Maßnahmen zu kombinieren und dadurch einen mehrschichtigen Sicherungsmechanismus zu etablieren.

III. Übersicht

Aufgrund der obigen Ausführungen sind folgende Punkte im Hinblick auf den Geheimnisschutz zu überprüfen:

- Sind sämtliche Arbeitsverträge auf dem aktuellen Stand?
- Sind Vertrags-Templates, insbesondere für NDAs auf dem aktuellen Stand? Enthalten diese eine Klausel zum Verbot des Reverse Engineering?
- Wie werden Geschäftsgeheimnisse in Ihrem Unternehmen geschützt? Existieren abgestufte Zugriffsberechtigungen?
- Wie wird der Schutz von Geschäftsgeheimnissen in Ihrem Unternehmen dokumentiert?
- Wie werden Mitarbeiter zum Thema Geheimnisschutz geschult?
- Ist es für Ihr Unternehmen sinnvoll, Klauseln zur Schiedsgerichtsbarkeit zu vereinbaren, um dem Risiko einer Offenlegung von Know-How in Gerichtsprozessen zu vermeiden?

Kontaktieren Sie uns, wir beraten Sie gerne!

Sarah Op den Camp
Rechtsanwältin
Fachanwältin für Handels-
Und Gesellschaftsrecht

Dr. Christopher Lieb, LL.M.Eur.
Rechtsanwalt
Fachanwalt für Handels- und
Gesellschaftsrecht