Rundschreiben | Dezember 2017

GEHEIMNISSCHUTZ-RICHTLINIE DER EU

von Jochen Sties und Dr. Adrian Kleinheyer

Warum es sich lohnt, dieses Rundscheiben zu lesen, auch wenn wir uns diesmal nicht kurzfassen konnten

Aufgrund der sogenannten Geheimnisschutz-Richtlinie der EU werden künftig nur solche Informationen als Geschäftsgeheimnisse oder Know-how anerkannt, die vom Unternehmen explizit vorab als vertraulich gekennzeichnet wurden und zu deren Schutz das Unternehmen angemessene Schutzmaßnahmen getroffen hat. Andernfalls kann man sich vor Gericht nicht wehren, falls Geschäftsgeheimnisse oder Know-how unbefugt erworben, verwendet oder weitergegeben wurden.

Hintergrund

Im Juli 2016 ist die *„Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung"* der EU (hier nachfolgend „Geheimnisschutz-Richtlinie") in Kraft getreten, mit der der Schutz von Geschäftsgeheimnissen und Know-how geregelt wird. Die Richtlinie muss bis Juli 2018 in deutsches Recht umgesetzt werden. Eigentlich wollten wir Sie über die Änderungen informieren, wenn konkret erkennbar ist, wie diese Umsetzung aussieht. Mittlerweile ist aber absehbar, dass die Richtlinie nicht rechtzeitig in deutsches Recht umgesetzt werden wird; es gibt bisher nicht einmal einen Gesetzesentwurf.

Aber auch ohne Umsetzung sind die Gerichte verpflichtet, die Geheimnisschutz-Richtlinie zu berücksichtigen, wenn auf der Basis der aktuellen Rechtslage über Streitfälle entschieden wird, die unter die Geheimnisschutz-Richtlinie fallen. Und die Auswirkungen in der Praxis werden

erheblich sein. Es müssen künftig im Vorfeld konkrete Maßnahmen getroffen werden, damit man aus dem ganzen „Werkzeugkasten" der rechtlichen Maßnahmen (z.B. Schadensersatz und Unterlassung) schöpfen kann, falls ein Dritter Geschäftsgeheimnisse und/ oder Know-how unbefugt verwendet oder an Wettbewerber weitergegeben hat.

Derzeitige Rechtslage

Vereinfacht zusammengefasst ist die unbefugte Verwertung von Geschäftsgeheimnissen oder Know-how oder deren Weitergabe an andere durch das UWG untersagt. Dabei ist die deutsche Rechtsprechung recht großzügig, was Geschäftsgeheimnisse oder Know-how sein können. Insbesondere muss ein Unternehmen nicht im Vorfeld angeben, was es als eigene Geschäftsgeheimnisse oder eigenes Know-how ansieht. Im Zweifel geht das Gericht davon aus, dass bestimmte Informationen vertraulich waren und dass das allen Beteiligten hätte klar sein müssen.

Außerdem ist nach derzeitiger deutscher Rechtsprechung Reverse Engineering nur dann zulässig, wenn jeder Fachmann dazu ohne großen Kosten- und Zeitaufwand in der Lage ist.

Änderung durch die Geheimnisschutz-Richtlinie

Durch die Geheimnisschutz-Richtlinie wird der Begriff des Geschäftsgeheimnisses genau definiert. Gemäß der Geheimnisschutz-Richtlinie ist ein Geschäftsgeheimnis/Know-how eine Information,

- die mit dem Geschäftsbetrieb im Zusammenhang steht,
- die nicht offenkundig ist,
- an deren Geheimhaltung das Unternehmen ein berechtigtes wirtschaftliches Interesse hat **und**
- die nach dem erklärten (oder wenigstens klar erkennbaren) Willen des Unternehmens geheim bleiben soll und zu deren Schutz das Unternehmen angemessene Schutzmaßnahmen ergriffen hat.

Nach dieser Definition muss jeder, der vertrauliche Informationen als Geschäftsgeheimnisse schützen möchte, im Vorfeld aktiv werden.

Künftig ist nur das ein Geschäftsgeheimnis oder Know-how, was ein Unternehmen aktiv als solches identifiziert hat. Hinzu kommt, dass das Unternehmen geeignete Schutzmaßnahmen ergriffen haben muss. Wenn im Streitfall nicht nachgewiesen werden kann, dass die weitergegebenen Informationen gegenüber den relevanten Mitarbeitern als Geschäftsgeheimnis oder Know-how identifiziert wurden und dass geeignete Schutzmaßnahmen ergriffen wurden, gewährt das Gesetz keinen Schutz für die Informationen.

Dies bedeutet in der Praxis eine faktische Umkehr der Beweislast gegenüber der derzeitigen Rechtslage.

Eine weitere Änderung betrifft das Reverse Engineering. Künftig ist Reverse Engineering grundsätzlich erlaubt, wenn das entsprechende Produkt rechtmäßig erworben wurde und das Reverse Engineering nicht vertraglich ausgeschlossen wurde (was aber nicht uneingeschränkt möglich sein soll).

Diese Änderungen bedeuten eine einschneidende Abweichung von der derzeitigen Rechtslage, so dass die bisher allgemein üblichen Maßnahmen in deutschen Unternehmen zum Geheimnisschutz nicht mehr ausreichen, um Schutz für ein Geschäftsgeheimnis zu erhalten.

Rechtliche Folgen bei Verstoß gegen Geheimhaltungspflicht

Wenn ein Unternehmen ein Produkt anbietet, das in erheblichem Umfang auf einem Geschäftsgeheimnis eines anderen beruht (z.B. hinsichtlich der Konstruktion, des Herstellungsverfahrens oder auch hinsichtlich des Marketings), hat der Verletzte nach geltendem Recht Anspruch auf

- Unterlassung (unter dem Vorbehalt der Verhältnismäßigkeit)
- Beseitigung
- Schadensersatz
- Auskunft

Durch die Geheimnisschutz-Richtlinie hinzu kommen Ansprüche auf Rückruf und Vernichtung; zudem wird die Durchsetzung insbesondere des Unterlassungs- und Beseitigungsanspruches deutlich vereinfacht. Denn diese Ansprüche sind nun unabhängig davon, ob dem Verletzer bekannt war, dass das von ihm angebotene Produkt ein Geschäftsgeheimnis eines anderen enthält. Dadurch wird die Verfolgung von Verletzern deutlich vereinfacht.

Ein Risiko, selbst Ziel von Forderungen zu werden, entsteht insbesondere bei neuen Mitarbeitern, falls diese aus ihrer früheren Tätigkeit (wissentlich oder unwissentlich) Informationen mitbringen, die ein für den früheren Arbeitgeber geschütztes Geschäftsgeheimnis oder geschütztes Know-how darstellen und diese Informationen in die Entwicklung von neuen Produkten beim neuen Arbeitgeber einfließen. Wenn der neue Arbeitgeber dies hätte erkennen müssen, „infiziert" die geschützte Information u.U. das ganze Produkt. Zwar verlangt die Geheimnisschutz-Richtlinie explizit, dass die „Nutzung von Erfahrungen und Fähigkeiten, die Arbeitnehmer im normalen Verlauf ihrer Tätigkeit ehrlich erworben haben", nicht beschränkt werden darf. Wie dieser Grundsatz konkret von Gerichten ausgelegt wird, muss sich aber erst noch zeigen.

Empfohlene Schritte für eigene Geschäftsgeheimnisse und eigenes Know-how

Es sind zwei unabhängige Maßnahmen erforderlich. Zum einen sollten Sie Ihren Umgang mit Geschäftsgeheimnissen anpassen, um Schutz entstehen zu lassen, und zum anderen sollten Sie aktuelle Vertragsbeziehungen anpassen, um Reverse Engineering auszuschließen.

Damit der Schutz nach der Geheimnisschutz-Richtlinie entsteht, sind vier Schritte nötig:

1. Geschäftsgeheimnisse/Know-how identifizieren,
2. die identifizierten Geschäftsgeheimnisse bzw. das identifizierte Know-how gegenüber den Mitarbeitern benennen,
3. Schutzmaßnahmen für diese Geschäftsgeheimnisse/Know-how ergreifen, und
4. Schutzmaßnahmen dokumentieren.

Zunächst müssen also Geschäftsgeheimnisse gefunden und bewertet werden. Dies können technische Zeichnungen, nicht-schriftliches Wissen (z.B. Passungen, Toleranzen) und kaufmännische Informationen sein.

Um Ihnen die Bewertung zu vereinfachen, was genau als Geschäftsgeheimnis angesehen werden sollte, haben wir Ihnen eine Checkliste mit weiteren Beispielen beigefügt.

Sind alle Geschäftsgeheimnisse identifiziert, muss den Mitarbeitern konkret mitgeteilt werden, was als Geschäftsgeheimnis betrachtet wird. Die Aufstellung muss regelmäßig aktualisiert werden.

Es muss nachweisbar sein, dass die zu schützenden Informationen den Mitarbeitern gegenüber als solche identifiziert wurden. Wir empfehlen eine schriftliche Aufstellung, deren Empfang vom Arbeitnehmer quittiert wird.

Außerdem müssen geeignete Schutzmaßnahmen ergriffen werden, die verhindern, dass die Geschäftsgeheimnisse in unbefugte Hände gelangen. Beispiele sind:

- Zugangskontrollen/-beschränkungen (sowohl physisch zu bestimmten Abteilungen, zum Prototypenbau, zum Musterlabor etc. als auch auf Netzwerkebene zu Projektdaten, Zeichnungen, Lieferantenlisten, etc.)
- Know-how für ein Projekt auf verschiedene Mitarbeiter aufteilen, so dass nicht einer allein alles weiß
- Überwachungsmaßnahmen, ob jemand auf Daten zugreift oder zuzugreifen versucht, die ihn eigentlich nichts angehen.

Im Streitfall muss nachgewiesen werden können, dass Schutzmaßnahmen ergriffen wurden und dass sie bezogen auf den Wert des jeweiligen Geschäftsgeheimnisses oder des Know-hows angemessen waren.

Daher sind eine lückenlose Dokumentation und eine regelmäßige Überprüfung unerlässlich. Außerdem müssen die Schutzmaßnahmen angepasst werden, beispielsweise wenn neue, technisch wirksamere Schutzmechanismen zur Verfügung stehen.

Unabhängig von der Identifikation der Geschäftsgeheimnisse sollten bestehende Geheimhaltungsverpflichtungen und Lieferverträge bei Kooperationen, bei denen Reverse Engineering unerwünscht ist, um eine Klausel ergänzt werden, die dies untersagt.

Zusammenfassung

Die Geheimnisschutz-Richtlinie wird für die meisten deutschen Unternehmen eine Änderung der Prozesse beim Umgang mit Know-how notwendig machen. Außerdem müssen Kooperations- und Lieferverträge angepasst werden.

Jochen Sties
Patentanwalt
j.sties@prinz.eu
089 / 59 98 87–103

Dr. Adrian Kleinheyer
Rechtsanwalt
a.kleinheyer@prinz.eu
089 / 59 98 87–107

FRAGEN?

Bei der Anpassung der Verträge können wir Sie gerne entlasten. Sie können hierzu Jochen Sties oder Dr. Adrian Kleinheyer jederzeit gerne ansprechen.

Dieses Rundschreiben stellt keine rechtliche Beratung dar und kann auch keine rechtliche Beratung für den Einzelfall ersetzen.

Prinz & Partner mbB
Rundfunkplatz 2
80335 München

Telefon: +49 (0) 89 / 59 98 87-0
Telefax: +49 (0) 89 / 59 98 87-211
E-Mail: info@prinz.eu

Checkliste

Geschäftsgeheimnisse identifizieren

Für die Entscheidung, ob eine bestimmte Information als Geschäftsgeheimnis geschützt werden sollte, eignen sich folgende Fragen:

- ✓ Ist die Information unternehmensbezogen?
- ✓ Ist die Information den relevanten Fachkreisen unbekannt?
- ✓ Ist die Information von wirtschaftlichem Wert?
- ✓ Entsteht der Wert der Information dadurch, dass sie geheim ist?

Wenn Sie alle Fragen mit „Ja" beantwortet haben, kann die infrage stehende Information als Geschäftsgeheimnis geschützt werden.

Für die Entscheidung, ob und in welchem Grad diese Information geschützt werden sollte, eignen sich folgende Fragen:

Wie groß ist der Schaden, wenn diese Information weitergegeben wird?

- ✓ Verheerend (z.B. gefährdet die Substanz des gesamten Unternehmens)
- ✓ Groß (z.B. gefährdet den Erfolg eines wichtigen Produkts)
- ✓ Mittel (z.B. verringert den Entwicklungs-/Kostenvorsprung gegenüber dem Wettbewerb)
- ✓ Gering (z.B. verkraftbare Gewinneinbuße)

Entsprechend des möglichen Schadens sollten unterschiedliche Schutzmaßnahmen ergriffen werden.

Bei Informationen, bei deren Veröffentlichung oder Weitergabe der Schaden verheerend wäre, muss der Zugriff auf den kleinstmöglichen Personenkreis beschränkt werden. Es kann auch angedacht werden, die Information nie einem einzelnen Mitarbeiter vollständig zur Verfügung zu stellen, sondern sie auf verschiedene Mitarbeiter aufzuteilen.

Bei Informationen, bei deren Veröffentlichung oder Weitergabe der Schaden gering oder mittel ist, sind folgende Überlegungen sinnvoll: In wie weit steht der Aufwand für den Schutz der Information und die sich aus den Schutzmaßnahmen ergebende Beeinträchtigung des normalen Geschäftsbetriebs in einem angemessenen Verhältnis zum eventuellen Schaden?

Beispiele für mögliche Geschäftsgeheimnisse

- Konstruktionsdetails (technische Zeichnungen)
- Know-how, das nicht schriftlich niedergelegt ist (z.B. die Auslegung von Spritzgussformen, Passungen, Toleranzen, bestimmte Werkstofflieferanten, verwendete Materialien, Temperaturführung bei Bearbeitungsprozessen, verwendete Werkzeuge und Schnittparameter bei der spanenden Bearbeitung)
- Kaufmännische Informationen (z.B. Kundenlisten, Kalkulationen, Preisgestaltungen, Strategien, Ausschreibungsunterlagen, Analysen von Wettbewerbern)

Prinz & Partner mbB
Rundfunkplatz 2
80335 München

Telefon: +49 (0) 89 / 59 98 87-0
Telefax: +49 (0) 89 / 59 98 87-211
E-Mail: info@prinz.eu