Know-how-Richtlinie

Neue Anforderungen an den Schutz von Geschäfts-geheimnissen

Die sogenannte Know-how-Richtlinie soll Unternehmen besser vor Geheimnisverrat und Wirtschaftsspionage schützen. Gleichzeitig stellt sie neue Anforderungen an den Schutz von Geschäftsgeheimnissen.

Die neue EU-Richtlinie zum Schutz von Geschäftsgeheimnissen und Know-how zielt darauf ab, Unternehmen vor Geheimnisverrat und Wirtschaftsspionage zu schützen und grenzüberschreitende Innovationen im europäischen Binnenmarkt zu fördern. Gleichzeitig stellt die Richtlinie neue Anforderungen an den Schutz von Geschäftsgeheimnissen. Es gilt: Die Richtlinie schützt nur den, der die Anforderungen erfüllt. Geschützt werden nur Informationen, die Gegenstand angemessener Geheimhaltungsmaßnahmen sind. Unternehmen müssen zukünftig beweisbare Geheimhaltungsmaßnahmen treffen, um Rechtsschutz zu erlangen.

Zweck der Richtlinie ist ein wirkungsvoller und europaweit einheitlicher Schutz vor Geheimnisverrat und Wirtschaftsspionage.

Worum geht es?

Im April 2016 hat das europäische Parlament die Richtlinie 2016/943 über den Schutz von Geschäftsgeheimnissen verabschiedet. Sie ist von den nationalen Gesetzgebern bis zum 9. Juni 2018 umzusetzen. Zweck der Richtlinie ist ein wirkungsvoller und europaweit einheitlicher Schutz vor Geheimnisverrat und Wirtschaftsspionage. Hierdurch sollen Anreize für grenzüberschreitende Kooperationen geschaffen und Europa als Wirtschafts- und Innovationsstandort gestärkt werden.

Hintergrund der Richtlinie ist folgender:

Zentrale Bedeutung von Geschäftsgeheimnissen
Für Unternehmen ist der Schutz von Geschäftsgeheimnissen von zentraler Bedeutung. Dies betrifft zum einen technische Innovationen und Know-how als entscheidende Faktoren für die Wettbewerbsfähigkeit und den Markterfolg von Unternehmen. Zum anderen besteht großes Interesse daran, vertrauliche kaufmännische Information, wie Kunden- und Lieferantendaten, Businesspläne, Bilanzen und Marktstrategien von der Öffentlichkeit und der Konkurrenz abzuschirmen.

Verschärfte Bedrohungslage
Der zentralen Bedeutung der Geschäftsgeheimnisse steht eine verschärfte Bedrohungslage gegenüber: Faktoren wie Globalisierung, Digitalisierung, Outsourcing, komplexere Geschäftsmodelle und längere Lieferketten erhöhen das Risiko, dass Dritte unbefugt Zugriff auf Geschäftsgeheimnisse erlangen.

Bisherige Situation
Geschäftsgeheimnisse sind bislang europaweit nicht einheitlich geschützt. Die nationalen Regelungen in den EU-Mitgliedsstaaten weisen erhebliche Unterschiede auf. In Deutschland gibt es bislang kein spezielles Gesetz für den Schutz von Geschäftsgeheimnissen. Die Regelungen sind über mehrere Gesetze verstreut. Nur in den Fällen, in denen Geschäftsgeheimisse als geistiges Eigentum geschützt sind, z.B. als Patente, Geschmacksmuster, Gebrauchsmuster oder urheberrechtliche Werke, besteht ein ausreichendes Maß an Rechtssicherheit. Mit der Richtlinie soll europaweit ein einheitlicher Rechtsschutz auf hohem Niveau gewährleistet werden.

Inhalt der Richtlinie

Kurz zusammengefasst sind folgende Inhalte der Richtlinie besonders interessant: Der Begriff des Geschäftsgeheimnisses wird in Artikel 2 Abs. 1 der Richtlinie neu definiert. Geschäftsgeheimnisse sind alle Informationen,

- die nicht allgemein bekannt oder ohne Weiteres zugänglich, also geheim sind und
- von kommerziellem Wert, weil sie geheim sind und
- Gegenstand angemessener Geheimhaltungsmaßnahmen des Geheimnisträgers sind.

Zudem legt die Richtlinie in den Artikeln 3 bis 5 fest, wann Erwerb, Nutzung und Offenlegung von Geschäftsgeheimnissen rechtmäßig und wann diese rechtswidrig sind. Wichtig für Unternehmen ist in diesem Zusammenhang, dass das Reverse Engineering, also die Untersuchung, Entschlüsselung oder der Rückbau eines öffentlich verfügbar gemachten oder rechtmäßig erworbenen Produkts, nun ausdrücklich als rechtmäßig erachtet wird. Werden Produkte über Reverse Engineering kopiert, bleibt in Zukunft wohl nur der Rückgriff auf gewerbliche Schutzrechte wie das Urheberrecht.

Weiterhin regelt die Richtlinie in den Artikeln 6 und 10 bis 15, welche Rechtsschutzmöglichkeiten für Inhaber von Geschäftsgeheimnissen bei rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung bestehen. Neben Unterlassung und Schadensersatz sollen weitere Maßnahmen wie Vernichtung, Rückruf, Beseitigung und Beschlagnahme gerichtlich durchgesetzt werden können. Neu ist, dass nach Artikel 14 Absatz 2 der Richtlinie die Höhe des Schadensersatzes nun auf zweifache Weise berechnet werden kann. Zum einen kann ein tatsächlich entstandener Schaden ersetzt werden. Die andere Möglichkeit der Berechnung orientiert sich daran, wieviel der Verletzer hätte zahlen müssen, um auf legalem Wege die vertrauliche Information zu erhalten oder zu nutzen (Lizenzanalogie). Dies erleichtert es Unternehmen, im Prozess einen Schadensersatzanspruch durchzusetzen, da ein konkreter Schaden im Falle der Lizenzanalogie nicht bewiesen werden muss.

Schließlich wird in Artikel 9 der Richtlinie der Umgang mit Geschäftsgeheimnissen in gerichtlichen Verfahren geregelt. Um zu verhindern, dass Geschäftsgeheimnisse im gerichtlichen Verfahren an die Öffentlichkeit gelangen, soll der Kreis derjenigen beschränkt werden, die Zugang zu solchen Verfahrensdokumenten oder Anhörungen haben, die Geschäftsgeheimnisse beinhalten.

Strengere Anforderungen an Geheimhaltungsmaßnahmen

Bislang sind Unternehmen im Wesentlichen durch § 17 des Gesetzes gegen Unlauteren Wettbewerb (UWG) vor Geheimnisverrat durch Beschäftigte während des Beschäftigungsverhältnisses und vor Wirtschaftsspionage geschützt. Nach dieser Vorschrift sind nicht offenkundige Betriebsinterna geschützt, wenn ein Geheimhaltungsinteresse besteht und ein Geheimhaltungswille erkennbar ist. Die Anforderungen der Gerichte an die Erkennbarkeit des Geheimhaltungswillens sind allerdings sehr gering. Ein solcher Wille wird im Regelfall vermutet, selbst wenn keine objektiven Geheimhaltungsmaßnahmen getroffen wurden.

Die neue Richtlinie geht einen anderen Weg. Wie bereits im Abschnitt „Inhalt der Richtlinie" dargestellt, liegt nach dem neuen Recht nur dann ein Geschäftsgeheimnis vor, wenn die betreffende Information Gegenstand angemessener Geheimhaltungsmaßnahmen des Geheimnisträgers ist. Dies hat zur Folge, dass Unternehmen in einem gerichtlichen Verfahren konkret vortragen und beweisen müssen, welche Geheimhaltungsmaßnahmen zum Schutz der jeweiligen Information getroffen wurden.

In welchem Fall welche Geheimhaltungsmaßnahmen angemessen sind, ergibt sich indes weder aus der Richtlinie, noch aus ihrer Begründung. Die konkrete Umsetzung der Richtlinie unterliegt daher einiger Rechtsunsicherheit. Jedoch ist davon auszugehen, dass das Rad nicht neu erfunden werden wird. Der nationale Gesetzgeber dürfte sich bei der Konkretisierung an Maßnahmen orientieren, die bereits aus dem IT- und Datenschutzbereich bekannt sind. Bei der Beurteilung der Frage, ob sie auch angemessen sind, ist im konkreten Einzelfall unter anderem auf die Schutzbedürftigkeit der vertraulichen Information und die drohenden Risiken abzustellen.

Mögliche Geheimhaltungsmaßnahmen

Mögliche objektive und beweisbare Maßnahmen zum Schutz von Geschäftsgeheimnissen können sowohl vertraglicher, als auch technischer und organisatorischer Art sein.

Vertragliche Geheimhaltungsmaßnahmen

Im Umgang mit Kooperationspartnern oder Dritten sind vertragliche Vertraulichkeitsvereinbarungen (Non-Disclosure Agreements) geeignete Maßnahmen zum Schutz von unternehmensinternen Geschäftsgeheimnissen und Know-how. Auch bei diesen Vereinbarungen ist es sinnvoll, den Schutzgegenstand klar abzugrenzen und erlaubte Nutzungen zu definieren. Zudem bietet es sich an, Vereinbarungen zur Rückgabe oder Vernichtung verkörperter Informationen nach dem Ende der Zusammenarbeit oder des Projekts zu schließen.

Um die Gefahren des Reverse Engineering zu reduzieren, kann Vertragspartnern der Nachbau des Produktes vertraglich untersagt werden. Ist Gegenstand des Vertrages eine Software, sind bei einem vertraglichen Reverse-Engineering-Verbot jedoch die Einschränkungen des Urhebergesetzes zu beachten, die bestimmte Formen des Beobachtens, Untersuchens und Testens von Computerprogrammen erlauben.

Auf vertraglicher Ebene sind auch arbeitsvertragliche Geheimhaltungsvereinbarungen ein wirksames

Mittel, um im Hinblick auf Beschäftigte im Unternehmen nicht offenkundige Betriebsinterna zu schützen. Bei der Formulierung entsprechender Klauseln ist darauf zu achten, dass diese ausreichend detailliert und differenziert sind und sich an den konkreten Geheimhaltungsinteressen des Unternehmens orientieren. Klauseln, die den Arbeitnehmer dazu verpflichten, über sämtliche betrieblichen Angelegenheiten Stillschweigen zu bewahren, sind nach der Rechtsprechung unwirksam. Nachvertragliche Wettbewerbsklauseln oder Klauseln, die zur Stillschweigen nach Beendigung des Arbeitsverhältnisses verpflichten, dürfen nach der Rechtsprechung überdies das berufliche Fortkommen des Beschäftigten nicht übermäßig beschränken.

Bei allen vertraglichen Vertraulichkeitsvereinbarungen ist dringend zu empfehlen, geeignete Rechtsfolgen im Falle von Vertraulichkeitsverletzungen zu formulieren. Sanktionsandrohungen schaffen wirksame Anreize für den Vertragspartner, seine Vertraulichkeitsverpflichtungen einzuhalten. Als Sanktionen sind insbesondere Vertragsstrafen und Kündigungsrechte denkbar.

Technische und organisatorische Geheimhaltungsmaßnahmen

Auf technischer und organisatorischer Ebene sind ebenfalls diverse Geheimhaltungsmaßnahmen denkbar, die aus den Bereichen Datenschutz und IT-Sicherheit bekannt sind. So sind Zutrittsbeschränkungen zum Unternehmensgelände und innerhalb des Unternehmens sinnvoll, um zu verhindern, dass Dritte unberechtigt Räumlichkeiten betreten. In digitaler Form gespeicherte Informationen sollten durch ausreichende Maßnahmen wie Zugangssperren oder eine abgesicherte Netzwerkarchitektur vor unbefugtem Zugang geschützt werden. Zudem sollte der Zugriff auf vertrauliche Informationen beschränkt sein auf Personen, die die Informationen zur Erfüllung ihrer Aufgaben benötigen. Hierzu können abgestufte Zugriffsberechtigungen vergeben werden, welche in einem entsprechenden Zugriffskonzept definiert sein sollten. Der Zugriff sollte zudem dokumentiert werden.

Die Weitergabe von vertraulichen Informationen innerhalb des Unternehmens oder an Dritte sollte ausreichend dokumentiert und kontrolliert werden. Sicherheitsmaßnahmen im Rahmen der Informationsweitergabe wie z.B. Verschlüsselung oder Passwortschutz können die Gefahr unberechtigten Zugriffs reduzieren. Auch ein Verbot der Nutzung privater Speichermedien kann eine geeignete Maßnahme sein, um zum einen die Sicherheit der IT-Systeme zu gewährleisten und zum anderen den unerwünschten Abfluss von Informationen zu verhindern, insbesondere bei Ausscheiden eines Mitarbeiters. Schließlich ist es sinnvoll, die Mitarbeiter mithilfe von Handreichungen oder Schulungen für die Thematik Schutz von Geschäftsgeheimnissen zu sensibilisieren. Um die Beweisführung im Prozess zu erleichtern, sollten sämtliche Geheimhaltungsmaßnahmen dokumentiert werden.

Schutzkonzept

Es kann sich anbieten, im Unternehmen ein Konzept zum Schutz von Geschäftsgeheimnissen zu etablieren, vergleichbar mit einem Informationssicherheitsmanagementsystem (ISMS) im Bereich IT-Sicherheit. Im Rahmen eines solchen Konzepts sollte zunächst evaluiert werden, welche Informationen im Unternehmen vorliegen und wie geheimhaltungsbedürftig sie sind. Sodann bietet es sich an, die Informationen nach ihrer Schutzbedürftigkeit zu strukturieren, Risiken zu evaluieren und zu überlegen, mit welchen Maßnahmen den Risiken begegnet werden kann. In die Entwicklung des Konzepts sollte auch die Frage einbezogen werden, ob bestimmte gesetzliche, vertragliche oder unternehmensinterne Anforderungen an den Schutz der Informationen bestehen. Ausgehend von den Ergebnissen dieser Inventarisierung, Strukturierung und Analyse kann ein Konzept erarbeitet werden, das konkrete technische und organisatorische Maßnahmen zum Schutz von vertraulichen Informationen vorsieht. Bei der Umsetzung des Konzepts ist es ratsam, Prozesse zu implementieren, mit denen Verletzungen des Geheimnisschutzes erkannt und analysiert werden können. Festgelegte Leitlinien zum Konzept bieten Beschäftigten des Unternehmens klare Vorgaben zum Umgang mit Geschäftsgeheimnissen. Bestehende Konzepte sollten laufend überprüft und verbessert werden. Um den Schutz der Geschäftsgeheimnisse vor Gericht beweisen zu können, empfiehlt es sich, das Konzept und die Maßnahmen schriftlich zu dokumentieren.

Themenübergreifendes Konzept und Management

Wie die Ausführungen zu den Geheimhaltungsmaßnahmen zeigen, besteht eine erhebliche Sachnähe zu den Anforderungen in den Bereichen Datenschutz und IT-Sicherheit. In der Praxis wird es vielfach zu Überschneidungen bei den Schutzmaßnahmen der jeweiligen Bereiche kommen. Vor diesem Hintergrund sollten Unternehmen erwägen, den Schutz von Informationen ganzheitlich und themenübergreifend anzugehen. Ein Gesamtkonzept bietet Unternehmen die Chance, durch kombinierte und einheitliche Herangehensweise Risiken zu minimieren, Entwicklungs- und Umsetzungsaufwand zu reduzieren und Prozesse zu optimieren.

Fazit

Die EU-Richtlinie zum Schutz von Geschäftsgeheimnissen und Know-how öffnet Raum für einen vereinfachten und verbesserten Schutz von Geschäftsgeheimnissen. Der damit einhergehenden Pflicht zum Einsatz angemessener Geheimhaltungsmaßnahmen können Unternehmen mit vertraglichen sowie technischen und organisatorischen Maßnahmen begegnen. Hierbei ist darauf zu achten, dass die Maßnahmen ausreichend dokumentiert werden, um Beweisschwierigkeiten zu vermeiden. Es bietet sich an, für die Bereiche Geheimnisschutz, Datenschutz und IT-Sicherheit ein einheitliches Konzept zu entwickeln und zu implementieren.

Die EU-Richtlinie zum Schutz von Geschäftsgeheimnissen und Know-how öffnet Raum für einen vereinfachten und verbesserten Schutz von Geschäftsgeheimnissen.

Ihr Ansprechpartner:

Dr. Söntje Julia Hilberg LL.M.
Head of IT-Law
Tel: +49 30 25468 228
Mobile: + 49 170 7663 353
Email: shilberg@deloitte.de

Mit redaktioneller Unterstützung von Maria Leutloff

Deloitte Legal Rechtsanwaltsgesellschaft mbH („Deloitte Legal") als verantwortliche Stelle i.S.d. BDSG ist die Rechtsberatungspraxis der Deloitte GmbH Wirtschaftsprüfungsgesellschaft („Deloitte"). Deloitte Legal und, soweit gesetzlich zulässig, Deloitte und die mit ihr verbundenen Unternehmen nutzen Ihre Daten im Rahmen individueller Vertragsbeziehungen sowie für eigene Marketingzwecke. Sie können der Verwendung Ihrer Daten für Marketingzwecke jederzeit durch entsprechende Mitteilung an Deloitte, Business Development, Kurfürstendamm 23, 10719 Berlin, oder kontakt@deloitte.de widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Deloitte Legal bezieht sich auf die Rechtsberatungspraxen der Mitgliedsunternehmen von Deloitte Touche Tohmatsu Limited, deren verbundene Unternehmen oder Partnerfirmen, die Rechtsdienstleistungen erbringen.
Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL"), eine „private company limited by guarantee" (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global" genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und ihren Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Steuerberatung, Financial Advisory und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen. Making an impact that matters – für mehr als 244.000 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen des Einzelfalls gerecht zu werden, und ist nicht dazu bestimmt, Grundlage für wirtschaftliche oder sonstige Entscheidungen zu sein. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk") erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.

Stand 12/2016