DR. FRITZ & COLL.

Whitepaper

Das Geschäftsgeheimnis – Was Unternehmen nun für deren Schutz unternehmen müssen

von Dr. Carmen Fritz, LL.M.
erstellt am 30.10.2019

Inhalte

Inhalt

Dieses Whitepaper wurde nach bestem Wissen und Gewissen erstellt. Er ersetzt jedoch nicht die anwaltliche Beratung im Einzelfall, sondern setzt lediglich Handlungsanreize bzw. stellt allgemeine Informationen zur Verfügung.

Einleitung

Zum 26.04.2019 trat das neue Geschäftsgeheimnisschutzgesetz in Kraft, welches nach nunmehr drei Jahren die „Richtlinie (EU) 2016/943 vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung“ umsetzt.

Die Dringlichkeit einer solchen einheitlichen Regelung ergab sich insbesondere aus dem Umstand, dass es bislang in den EU-Ländern unterschiedliche, missverständliche oder - wie in Deutschland - gar keine gesetzlichen Definitionen des Geschäftsgeheimnisbegriffs gab.
Das deutsche Gesetz gegen den Unlauteren Wettbewerb regelte bislang zwar in § 17 die Strafbarkeit des Geschäftsgeheimnisverrats, eine Definition des Begriffs des Geschäftsgeheimnisses enthält die Norm hingegen nicht. Vielmehr entwickelte die deutsche Rechtsprechung und Literatur über die Jahre eine Definition, über die mittlerweile weitestgehend Einigkeit besteht. Danach ist ein Geschäftsgeheimnis jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und an deren Geheimhaltung der Unternehmensinhaber ein berechtigtes wirtschaftliches Interesse hat und nach dem bekundeten, auf wirtschaftlichen Interessen beruhenden Willen des Betriebsinhabers geheim gehalten werden soll. Aufgrund der hohen Beweisschwierigkeit hinsichtlich des Geheimhaltungswillens führte diese Definition in der Vergangenheit regelmäßig zu unbefriedigenden Ergebnissen für die Inhaber von Geschäftsgeheimnissen.

Warum ist der Schutz wichtig?
Nach einem Studienbericht der bitkom aus dem Jahr 2015 waren 51 % der Unternehmen in den zwei Jahren davor von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffen, wodurch den Unternehmen ein Schaden von 51 Milliarden Euro pro Jahr entstand. Bei der Hälfte der Fälle war ein aktueller oder ehemaliger Mitarbeiter das Einfallstor, wobei diese sich dessen oftmals gar nicht bewusst waren.[1]

Geschäftsgeheimnisse sind auf vielfältige Art und Weise gefährdet

- durch Arbeitnehmerwechsel, Fluktuation
- Technologietransfers im Rahmen der Kooperation mit anderen Unternehmen
- Industriespionage
- Schäden durch Geheimnisabfluss

[1] Studie siehe unter https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf.

Geschäftsgeheimnis als komplexe Querschnittsmaterie

Beim Geheimnisschutzrecht handelt es sich um eine Querschnittsmaterie, welche Kenntnisse im Gewerblichen Rechtsschutz (v.a. Schutzrechte, Wettbewerbsrecht), im Vertragsrecht und im Arbeitsrecht verlangt.

I. Was ist neu beim Geschäftsgeheimnisschutz?

Unternehmen können nach dem neuen GeschGehG wie zuvor gegen unerlaubte Erlangung, Nutzung oder Offenbarung von Geschäftsgeheimnissen vorgehen; bei schweren Verstößen drohen weiterhin strafrechtliche Konsequenzen.

1. Überblick

Neu ist die viel diskutierte Privilegierung für Hinweisgeber („**Whistleblower**"), die gesetzliche Gestattung des sogenannten „**Reverse Engineering**" sowie die gesetzliche Konkretisierung der einzelnen Ansprüche, aber auch spezielle Verfahrensvorschriften, die die Geheimhaltung im gerichtlichen Verfahren sicherstellen, und der nun erstmals gesetzlich definierte – und im Vergleich zur bisherigen Rechtslage geänderte! – **Begriff des Geschäftsgeheimnisses**.

Mit dem neuen Begriff des Geschäftsgeheimisses geht aber auch die Umkehr der Beweislast einher, d.h. wer ein Geschäftsgeheimnis darlegt, muss jetzt nachweisen dass er sich betriebsintern darum bemüht hat, Maßnahmen einzuführen.

2. Durchsetzbare Ansprüche

Das GeschGehG schützt nunmehr anders als früher auf der zivilrechtlichen Ebene durch zahlreiche Ansprüche:

- Unterlassung
- Beseitigung einer Beeinträchtigung
- Vernichtung und/oder Herausgabe von Geheimnisträgern und vorhandener Kopien
- Rückruf eines rechtsverletzenden Produktes sowie Entfernung und Rücknahme eines rechtsverletzenden Produkts aus den Vertriebswegen.
- Auskunft
- Schadensersatz in Form des konkreten Schadens, des Verletzergewinns oder einer fiktiven Lizenz
- Ersatz eines Nichtvermögensschadens (Geldentschädigung)

Achtung: Das GeschGehG gibt nicht nur gegen den Rechtsverletzer einen Anspruch, sondern auch gegen den Inhaber des Unternehmens, sofern der Rechtsverletzer die Verletzungshandlung in einem unmittelbaren inneren Zusammenhang mit den von ihm wahrgenommenen Aufgaben im Unternehmen begangen hat.

Auf der strafrechtlichen Ebene nimmt das GeschGehG die bisherigen Strafvorschriften des UWG weitgehend auf und stellt Rechtsverletzungen unter Geldstrafe bzw. Freiheitsstrafe von bis zu fünf Jahren.

Da der Inhaber eines Geschäftsgeheimnisses bislang bei gerichtlicher Geltendmachung aufgrund des Grundsatzes der Öffentlichkeit immer auch das Risiko einging, das sein Geheimnis den Schutz verliert oder offengelegt wird, hat das GeschGehG auch hier angesetzt und neue Verfahrensvorschriften geschaffen. So können solche Verfahren gegen den/die Rechtsverletzer nunmehr auch unter Ausschluss der Öffentlichkeit durchgeführt werden. Dies gilt sowohl in den Verfahren vor der ordentlichen Gerichtsbarkeit als auch in Arbeitsgerichtsverfahren.

Neben dem GeschGehG bleiben natürlich die bisher vorgesehenen Tatbestände weiter bestehen. Geheimhaltungspflichten bestehen daher

a) im Stadium der Vertragsanbahnung, § 311 Abs. 2 BGB
b) sowie im nachvertraglichen Bereich, bspw. bei Abschluss eines nachvertraglichen Wettbewerbsverbots
c) im arbeitsvertraglichen Bereich aus Nebenpflicht gem. § 241 Abs. 2 BGB

Daneben bestehen gesetzliche Geheimhaltungspflichten, bspw. gem. § 93 I S. 3 AktG, § 79 BetrVG, § 13 Nr. 3 BBiG, § 24 Abs. 2 ArbNErfG, § 90 HGB

3. Reverse Engineering

Grundsätzlich ist Reverse Engineering erlaubt. Allerdings kann dies durch vertragliche Gestaltung untersagt werden. Das Problem beim Reverse Engineering ist, das derjenige, der ein Interesse daran hat über einen Rückbau Informationen zu gewinnen, in der Regel nicht der unmittelbare Vertragspartner ist. Dementsprechend muss sich das vertragliche Verbot über die gesamte Lieferkette mit Hilfe von Lizenzunterlassungsvereinbarungen aufrechterhalten. Hier kommt aber natürlich dem Patentschutz noch besondere Bedeutung zu.

II. Was ist denn nun ein Geschäftsgeheimnis?

GEHEIM IST NUR NOCH, WAS OBJEKTIV ANGEMESSEN GESCHÜTZT IST.

Nach § 2 Nr. 1 des GeschGehG ist ein Geschäftsgeheimnis nun eine

- ✓ Information
- ✓ die weder allgemein bekannt oder ohne Weiteres zugänglich ist (geheim) und
- ✓ von wirtschaftlichem Wert ist und
- ✓ die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
- ✓ bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Abzugrenzen ist das Geschäftsgeheimnis demnach von Privatgeheimnissen.
„Information“ bezeichnet jedes wettbewerbsrelevante und existentielle Wissen im Unternehmen. Dies umfasst nicht nur technologisches Wissen und technische Erfahrung oder Prozesse sondern eben auch Kunden- und Lieferanteninformationen, Businesspläne, Marketingstrategien, Wettbewerbsmarktanalysen, Personale Strukturierungskonzepte, Verhaltensdaten, Produktspezifikationen, Preise, Kalkulation von Angeboten, technische Erfindungen, Herstellungsverfahren, Prototypen, Formeln und Rezepte, Geschäftsstrategien, Unternehmensdaten etc.

Geheim ist nach der Geheimnisschutz-Richtlinie eine Information dann, wenn sie weder in Ihrer Gesamtheit noch in der genauen Anordnung oder Zusammensetzung ihrer Bestandteile den Personen, die üblicherweise mit dieser Art von Information umgehend, allgemein bekannt oder ohne weiteres zugänglich ist, vgl. Art. 2 Nr. 1 lit. a). Dies setzt den Geheimhaltungswillen des Inhabers des Geschäftsgeheimnisses voraus. Zum anderen darf eine Information nicht ohne größeren Zeit- oder Kostenaufwand zugänglich sein.

Existieren keine Kontrollmechanismen oder sind diese faktisch funktionslos, so dass die Information dem beliebigen Zugriff Dritter preisgegeben ist, ist die Information nicht mehr geheim.

Unter **wirtschaftlichem Wert** versteht man sowohl den realen als auch den potentiellen Handelswert einer solchen Information. Informationen die ohnehin leicht zugänglich, generell bekannt oder belanglos sind, werden daher vom Geschäftsgeheimnis nicht erfasst. Demnach liegt ein wirtschaftlicher Wert vor, wenn die Erlangung, Nutzung oder Offenlegung der entsprechenden Information ohne Zustimmung des Inhabers dessen wissenschaftliches oder technisches Potenzial, geschäftliche oder finanzielle Interesse, strategische Position oder Wettbewerbsfähigkeit negativ beeinflusst.

Angemessene Geheimhaltungsmaßnahmen sind Vorgänge, Prozesse oder Strategien, mit denen Unternehmen Vorgänge identifizieren oder klassifizieren, um sie zu schützen. Ähnlich dem TRIPS[2] sind daher technische und physische Sicherheitsvorkehrungen, vertragliche Vereinbarungen, Anweisungen, Belehrungen zu treffen und Dokumente mit Geheimhaltungshinweisen zu versehen. Die Geheimhaltungsmaßnahmen müssen angemessen sein. Die Gesetzesbegründung zum GeschGehG nennt sieben Kriterien:

- der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten
- die Natur der Information
- die Bedeutung für das Unternehmen
- die Größe des Unternehmens,
- die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen
- die Art der Kennzeichnung der Informationen und
- vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern.

Der Inhaber des Geschäftsgeheimnisses ist für das Vorliegen solcher Maßnahmen in Bezug auf das konkrete Geheimnis beweisbelastet.

Das **berechtigte Interesse** ist anhand objektiver Kriterien zu beantworten. Es ist daher nicht jedes rein wirtschaftliches Interesse gemeint. Gemeint sind bspw. technologisches Wissen, Rezepturen, Einkaufsbedingungen mit Lieferanten, marktspezifisches Erfahrungswissen, personenbezogene Daten von Kunden oder Lieferanten usw. Die Angemessenheit muss sich zunächst einmal auf den Wert des Geschäftsgeheimnisses im Verhältnis zum Unternehmen beziehen.

[2] Übereinkommen über handelsbezogene Aspekte der Recht4e des geistigen Eigentums.

Mögliche Geschäftsgeheimnisse[3] sind:

- ✓ Absatzgebiete
- ✓ Adressenverzeichnisse
- ✓ Ausschreibungsunterlagen
- ✓ Bezugsquellen
- ✓ Bieterlisten
- ✓ Buchführungsunterlagen
- ✓ Computerprogramme
- ✓ Entwürfe
- ✓ Formeln
- ✓ Geschäftsbücher und –briefe
- ✓ Geschäftsstrategien
- ✓ Herstellungsverfahren
- ✓ Kalkulationen
- ✓ Konstruktionsdaten
- ✓ Kostenansätze
- ✓ Kunden- und Lieferantenlisten
- ✓ Marktanalysen
- ✓ Muster
- ✓ Preisberechnungen
- ✓ Produktionsanlagen
- ✓ Prototypen
- ✓ Rezepte
- ✓ Schaltpläne
- ✓ Stoffzusammensetzungen
- ✓ Technische Zusammensetzungen
- ✓ Umsatzzahlen
- ✓ Unternehmensdaten
- ✓ Verschlüsselungssysteme

[3] Weitere vgl. unter Roland Reinfeld, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, S. 48 ff.

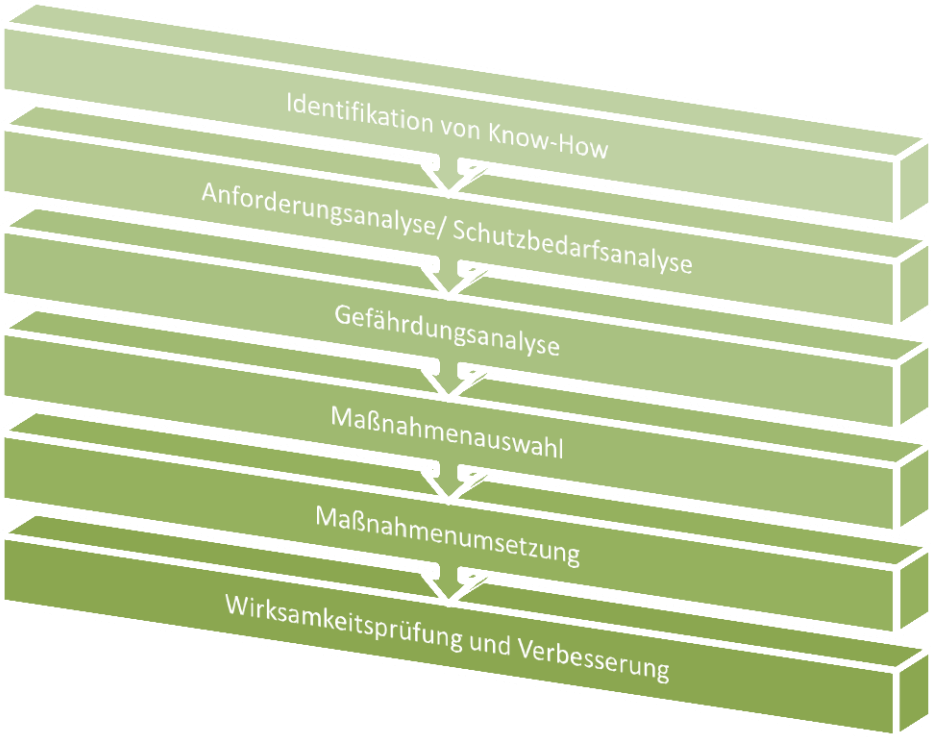
III. Wie schütze ich Geschäftsgeheimnisse?

Die neue Definition des Geschäftsgeheimnisses enthält ein bisher im deutschen Recht nicht vorhandenes Kriterium - das **Vorliegen angemessener Geheimhaltungsmaßnahmen** durch den Geheimnisinhaber. Unternehmen müssen nun aktiv werden, damit ihr schützenswertes Know-how vom Schutz des neuen Gesetzes profitiert. Für den Geschäftsinhaber bedeutet dies nunmehr vor allem, Vorgänge, Prozesse und Strategien zu entwickeln, um wirtschaftlich wertvolle Informationen vor unberechtigten Handlungen oder Eingriffen zu schützen. Für die Umsetzung des Schutzes bedarf es eines strukturierten Vorgehens durch das Unternehmen. Es gibt hierfür keine allgemein gültige Lösung – jedes Unternehmen muss eine eigene Lösung entwickeln.[4]

1. Zuständigkeit

Die Umsetzung fällt grundsätzlich in die Zuständigkeit der Unternehmensleitung und sollte alle Abteilungen, insbesondere die Rechtsabteilung, die Personalabteilung sowie die IT- und Konzernsicherheit mit einbeziehen.

2. Umsetzung

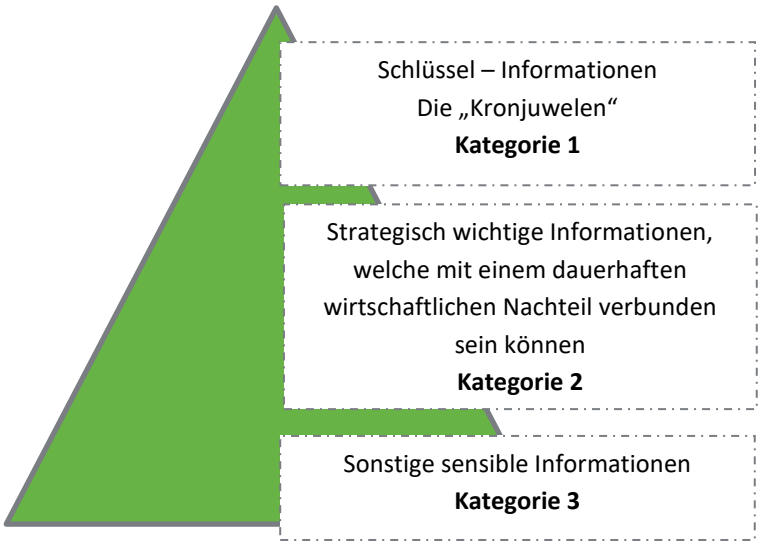


[4] Interessante Lektüre und Anregungen hierzu geben die Verschlusssachenanweisungen des Bundes ansehen

a) Identifizierung

Zunächst sind alle relevanten Personen, Verantwortlichkeiten und Abläufe zu identifizieren, d.h. die zu schützende Information muss geheim und wirtschaftlich wertvoll sein. Dies ist dann der Fall, wenn sie dem Geheimnisträger einen Wettbewerbsvorteil verschafft. Demzufolge muss das Unternehmen eine Bestandsaufnahme machen und wissen welche Informationen es aus welchem Grund geheim halten will. Es ist sodann der individuelle Wert festzulegen.

In diesem Zusammenhang sind alle Informationen formal zu erfassen und eine wirtschaftliche Bewertung vorzunehmen. Diese hat zu berücksichtigen, welche Erträge oder Einsparungen das Geheimnis erbringt, welcher sonstige Nutzen mit dem Geheimnis verbunden ist und welcher Aufwand einem Dritten für die Nachentwicklung oder den Zukauf von Alternativen entsteht.[5] Hierzu gibt es oftmals drei Kategorien:



b) Anforderungsanalyse/Schutzbedarfsfeststellung

Nun sollte man alle relevanten Anforderungen (DIN- oder ISO-Normen, Gesetze etc.) betrachten. Dies gilt aus folgender Sicht:

- ✓ Geschäftsprozessanforderungen
- ✓ Kundenanforderungen (etwa aufgrund von NDA´s)
- ✓ Lieferantenanforderungen (bspw. aufgrund von Kennzeichnungspflichten)

c) Gefährdungsanalyse

Hierzu zählt bereits die Konkurrenz sowie Wirtschaftsspionage, Wirtschaftskriminalität, IT- und Cybervorfälle, Human Risks etc.

d) Maßnahmenauswahl/umsetzung

Es sollten dringend Maßnahmen zur Vermeidung und/oder Verminderung der Risiken beschrieben werden und zwar im Rahmen eines Schutzkonzeptes als Kombination von

[5] vgl. Roland Reinfeld, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, S. 56.

organisatorischen, rechtlichen, personellen, technischen und kommunikativen Maßnahmen. Weiteres hierzu unter Punkt IV.

e) Wirksamkeitsprüfung und Verbesserung

Dabei erfordert das Ganze immer wieder eine Anpassung und Entwicklung neuer Maßnahmen sowie eine Kontrolle und kontinuierliche Nachbesserung. Insbesondere sollte immer im Normalbetrieb geprüft werden, ob die angestrebte Wirkung erzielt wird oder schlichtweg einfach auch unverhältnismäßig ist. In dem Fall muss sie angepasst oder ersetzt werden.

3. Checkliste: Anwendbarkeit des GeschGehG

Frage	*Ja*	*Nein*
Verfügt Ihr Unternehmen über exklusives Wissen, d.h. ist dieses Wissen weder allgemein bekannt noch ohne weiteres für jedermann zugänglich?		
Ist das Wissen in einem internen Verzeichnis bereits systematisch nach Kategorien (z.B. technisch/kaufmännisch) sowie weiteren Unterkategorien erfasst worden?		
Wurden die gesamten Wertschöpfungsprozesse in Ihrem Unternehmen systematisch auf potentiell vorhandene Besonderheiten und Alleinstellungsmerkmale analysiert?		
Ist das Wissen insbesondere nach Schutzklassen (z.B. „vertraulich“, „geheim“ und „streng geheim“) klassifiziert worden?		
Sind die Risiken der unerlaubten Erlangung, Nutzung und Offenlegung bei der Implementierung des Sicherheitskonzeptes berücksichtigt worden?		
Ergibt sich der jeweilige Informationswert gerade aus der Exklusivität der Information, d.h. besteht wegen der Alleinstellungsposition ein Vorteil gegenüber Wettbewerbern?		
Existieren bereits interne und/oder externe Zugriffsbeschränkungen in Bezug auf diese Informationen?		
Existiert in Ihrem Unternehmen ein Informationsschutzkonzept, das alle unternehmerischen Bereiche in Bezug auf geheimhaltungsbedürftige Informationen umfasst?		
Haben Sie durch schriftliche Anweisung Ihre Richtlinien zum Geheimnisschutz konkretisiert?		
Gibt es einen Sicherheitsverantwortlichen, der als zentraler Ansprechpartner und Koordinator für sämtliche Fragen des Geheimnisschutzes zuständig ist?		
Werden Hinweise auf Informationsverluste systematisch erfasst und analysiert?		
Enthalten die Arbeitsverträge individuelle Geheimhaltungsklauseln im Hinblick auf die Nutzung von Geschäftsgeheimnissen?		
Betreibt Ihr Unternehmen Markt-/Konkurrenzbeobachtung, um möglichst frühzeitig Hinweise auf Informationsverluste zu erhalten?		

IV. Schutzmaßnahmen

1. Organisatorische Maßnahmen

Der Begriff der technischen und organisatorischen Maßnahmen ist bereits aus dem Datenschutzrecht bekannt. Das Prinzip ist das Gleiche.

Ein wichtiges Beispiel hierfür ist die Einführung bzw. der Ausbau eines Berechtigungskonzepts nach dem Need-to-know-Prinzip:
Typischer Weise müssen Geschäftsgeheimnisse nur denjenigen Mitarbeitern bekannt sein, die mit Ihnen arbeiten; allen anderen sollten diese unbekannt sein. HR-Abteilungen sollten daher mit der Aufgabe vertraut werden, bei Einstellung und Freistellung auf das Geschäftsgeheimnis hinzuweisen und die Rückgabe von Dokumenten und Speichermedien zu überwachen und zu dokumentieren. Dies gilt auch für Kooperations- und Vertragspartner oder fremde Arbeitskräfte im Rahmen der Arbeitnehmerüberlassung.
Dabei sollte man sich bestimmte Fragen stellen:

- ✓ In welchen Organisationsbereichen wird mit welcher Art von Informationen gearbeitet?
- ✓ Welche Person benötigt Zugang zu welchen Informationen?
- ✓ Können derzeit andere Mitarbeiter aus anderen Organisationsbereichen oder fremde Unternehmen auf die Informationen zugreifen?

Weitere Maßnahmen sollten Zugangs-, Zutritts- und Nutzungsbeschränkungen sein – sowohl für Unternehmensfremde als auch für eigene Mitarbeiter.

2. Technische Maßnahmen

Diese Maßnahmen sind v.a. im Bereich der IT angesiedelt.

Zu denken sind hierbei v.a. an Zugriffsbeschränkungen und IT-Sicherheit (bspw. Netzwerksicherheit, Sicherheitsanalysen, Virenschutz, Aufrüstung, Updates, Verschlüsselungen, Erstellung von IT-Sicherheitsrichtlinien, rückstandsfreie Löschung von Datenträgern etc.

Dabei sind immer die jeweiligen technischen Möglichkeiten („Stand der Technik") der Maßstab. Ein vollkommener Schutz ist nicht möglich.

3. Vertragliche Maßnahmen

a) Mit Geschäftspartnern

Die sogenannte Vertraulichkeitsvereinbarung – NDA (Non-Disclosure Agreement) bietet insoweit Schutz, als mit Geschäftspartnern Vereinbarungen über die Vertraulichkeit geschlossen werden. Im Rahmen einer Zusammenarbeit bleibt es oftmals unvermeidbar, dass auch Geschäftsgeheimnisse offen gelegt werden. Daher ist es wichtig, bereits in einem frühen Stadium eine Vertraulichkeitsvereinbarung zu schließen. In der Regel ist daher die NDA das erste Dokument, welches die Parteien unterzeichnen. Eine NDA kann sowohl einseitig als auch zweiseitig verpflichtend geschlossen werden.

Inhaltlich ist von der Anfertigung und Verwendung von sogenannten Global oder general purpose – NDA ausdrücklich abzuraten; vielmehr sollte der Schutzgegenstand und der Schutzumfang oder auch der Zweck genau beschrieben werden und die NDA möglichst auf die Parteienkonstellation angepasst werden.

Wir empfehlen daher weder die Verwendung eines Standardmusters noch die Nutzung von Mustern aus dem Internet. Die Klauseln sind individuell zu verfassen und an vertragsrechtlichen Wirksamkeitsvoraussetzungen zu messen, welche viele Muster aus dem Internet nicht einhalten.

b) Mit Arbeitnehmern

Die Frage des Geheimnisschutzes stellt sich nicht nur im bestehenden Arbeitsverhältnis sondern auch im Rahmen von dessen Beendigung, bspw. wenn der Mitarbeiter zur Konkurrenz wechselt. Der Mitarbeiter wird regelmäßig ein Interesse daran haben, vorhandenes Wissen und Know-how weiter anwenden zu können. Dementsprechend fällt gerade Mitarbeitern die Abgrenzung zwischen Geschäftsgeheimnis und dem eigenen Erfahrungsschatz, den diese ja verwenden dürfen, sehr schwer.

Auch hier verbietet sich eine pauschale Regelung zur Geheimhaltungsverpflichtung getreu dem Motto „Catch-all“. Diese sind mangels Konkretisierung unwirksam. Die Maßnahmen müssen sich konkret auf die jeweiligen Geheimnisse beziehen.

Hierbei sind vor allem auch die Besonderheiten des Arbeitsrechts zu berücksichtigen, wonach die Klausel den Arbeitnehmer nicht unangemessen benachteiligen darf, hinreichend transparent sein muss und nicht vom wesentlichen Grundgedanken gesetzlicher Regelungen abweichen darf. Die alte Rechtslage setzte meistens voraus, dass es sich bei der Information bereits um ein Geschäftsgeheimnis handelte.

Die alten Klauseln, die sie in Arbeitsverträgen finden, sind mitunter daher nicht mehr geeignet, den neuen Geschäftsgeheimnisschutz umzusetzen. Wir empfehlen daher, neue Regelungen abzuschließen, insbesondere waren viele Klauseln in der Vergangenheit unwirksam, da man auch hier versuchte von den Arbeitnehmern alle betrieblichen Geheimnisse geheim halten zu lassen.

Des Weiteren sollte man darauf achten, dass eine betriebseinheitliche Klausel nicht mit individuellen Einzelvereinbarungen kollidiert.

Die Nutzung des eigenen Erfahrungsschatzes kann nicht untersagt werden, auch dann nicht, wenn es sich um spezialisiertes Wissen handelt, welches über einen längeren Zeitraum in herausgehobener Position erworben wurde.

Bei den Wettbewerbsverboten können vielerlei Fehler gemacht werden; deswegen empfehlen wir, diese in die Hände eines Anwalts zu legen. Mit einem Wettbewerbsverbot geht bspw. immer die Zahlung einer Karenzentschädigung einher; andernfalls sind diese Klauseln - soweit sie nachvertraglich gelten sollen - unwirksam. Ohne eine solche Klausel darf der Arbeitnehmer nachvertraglich konkurrieren – wenn auch ohne Verwertung des Geschäftsgeheimnisses.

Geheimhaltungsmaßnahmen, die offensichtlich rechtsunwirksam sind, sind keine angemessenen Geheimhaltungsmaßnahmen!!!!!

Die Verschwiegenheitsverpflichtung sollte die geheimhaltungsbedürftigen Informationen explizit benennen bzw. möglichst konkret umschreiben und eine hinreichend klare

Differenzierung zu sonstigen betrieblichen Vorgängen erkennen lassen. In zeitlicher Hinsicht gilt die Verschwiegenheitsverpflichtung grundsätzlich unbegrenzt (der BGH begrenzt die Verpflichtung auf die Dauer des Dienstverhältnisses), während das Wettbewerbsverbot auf einen Zeitraum von max. 2 Jahren beschränkt ist (vergl. § 74 a Abs. 1 HGB).

Empfehlenswert ist es beispielsweise, dem Arbeitsvertrag eine Anlage beizufügen, die die wesentlichen Pflichten im Zusammenhang mit dem Schutz von Geschäftsgeheimnissen aufzeigt.

4. Checkliste

a) Organisatorische Schutzmaßnahmen	
Verantwortung für das Informationsmanagement (Geheimnisbeauftragter) festgelegt.	
Kennzeichnung/Klassifikation vorhandener Informationen als Geschäftsgeheimnis ist erfolgt bzw. angewiesen (Erstellung eines „Inventars"/"Trade Secret Registry")	
Regeln und Dokumentationsmechanismen für den Zugang zu Geschäftsgeheimnissen sind etabliert (Listen, IT-Protokolle etc.)	
Ablaufplan für Schutz und Rechtsdurchsetzung im Fall von Verstößen gegen das GeschGehG aufgestellt	
Arbeitsteilige Prozesse auf Geheimnisschutz werden geprüft	
Begrenzung des Informationszugangs auf „Need-to-know"-Basis	
Besucherregelungen (bspw. Voranmeldung, Dokumentation der Teilnehmer bei Meetings, Umgang mit Mobiltelefonen, Abholung der Besucher durch Mitarbeiter, Aufnahme von Fotos etc.)	
Notfallplan mit internen Berichtsketten bei drohendem Know-how Verlust	
b) Rechtliche Schmutzmaßnahmen	
Verträge mit Mitarbeitern wurden in Bezug auf die Verschwiegenheitsklauseln kontrolliert und angepasst.	
Verträge mit Dienstleistern, Kunden und Kooperationspartnern enthalten angemessene Verschwiegenheitsklauseln und Verbot zum Reverse Engineering	
Interne Richtlinie mit Hinweisen auf gesetzliche Geheimhaltungspflichten in Arbeitsverträgen, Betriebsvereinbarungen etc. etabliert	
Detaillierte Vertraulichkeitsvereinbarungen (NDA) in kritischen/unternehmensrelevanten Prozessen sind getroffen und deren Einhaltung wird überwacht	
Frühzeitige Durchsetzung bei Verletzung (standardmäßig: direkte Klageerhebung nebst Antrag auf Durchführung des Klageverfahrens als Geheimnisschutzstreitsache)	
c) Personelle Schutzmaßnahmen	
Information der Mitarbeiter über Notwendigkeit des Schutzes von Geschäftsgeheimnissen	
Nachweis der Kenntnis darüber (Abgabe einer Erklärung durch den Mitarbeiter)	
Sorgfältige Auswahl des zugangsberechtigten Personals und Reduzierung der Zugangsberechtigungen auf das notwendige Maß	
Debriefing bei Beendigung des Arbeitsverhältnisses oder Wechsel des Arbeitsplatzes (Einführung von „EXIT-Gesprächen")	
Melde- bzw. Vergütungssysteme für neue Geheimnisse etabliert	

Clean-Desk-Policy	
Schulungen der Mitarbeiter	
d) Technische (und bauliche) Schutzmaßnahmen	
Berechtigungskonzepte für die relevanten IT-Systeme ist umgesetzt	
Absicherung des Geländes	
Trennung der Netzwerke	
Räumliche Abtrennung kritischer Bereiche, bspw. Forschung und Entwicklung vom Besucherbereich (deutliche Kennzeichnung der Räume mit Zutrittsverboten)	
IT-Sicherheit/ISMS nach ISO 27001 eingerichtet	
Werkschutz (Sicherheitspersonal, Zugangskarten)	
Verschlüsselte Kommunikation (verschlüsselte E-Mails; verschlüsselte Dokumente)	

Kontaktinformationen

Als Fachanwältin für Gewerblichen Rechtsschutz bieten wir Ihnen die bestmögliche Kompetenz.

Bei Fragen freuen wir uns über Ihre Kontaktaufnahme.

Ihre Ansprechpartner:

Dr. Carmen Fritz, LL.M.
Fachanwältin für Urheber- und Medienrecht
Fachanwältin für Gewerblichen Rechtsschutz
Fachanwältin für IT-Recht

DR. FRITZ &COLL.

Kanzlei Dr. Fritz
Poststr. 4
D-87435 Kempten
T: 0049 831/930 6564-0
E: kontakt@kanzlei-fritz.com
W: www.kanzlei-fritz.com