

Luther.

Know-how Richtlinie und Geheimnisschutz- gesetz

The background of the slide features a dark, blurred grid of white and green characters. The word "SECRET" is prominently displayed in a bright green, pixelated font across the lower half of the image. Other letters like "A", "B", "C", "D", "Y", "Z" are visible in a lighter, greyish-white color, creating a digital or data-themed aesthetic.

Inhalt

Know-how-Richtlinie und Geheimnisschutz

Seite 3

Status Quo des Know-how-Schutzes

Seite 6

Know-how-Richtlinie

Seite 7

Geschäftsgeheimnisgesetz

Seite 9

Ansprechpartner

Seite 22

Ein Kurzprofil von Luther

Seite 23

Auszeichnungen

Seite 24

Bedeutung von Know-how für Unternehmen

Know-how, also unternehmenskritisches Wissen, ist das Herzstück eines jeden Unternehmens. Neue Entwicklungen resultieren nicht selten aus dem bereits vorhandenen, unternehmensinternen Wissen.

Auch der Vorsprung zu Wettbewerbern liegt oftmals in geheimen Informationen, wie in Bauplänen, Konstruktionszeichnungen oder Rezepturen. Aber auch wichtige betriebswirtschaftliche Informationen, wie Kunden- oder Preislisten, haben in Unternehmen einen enormen wirtschaftlichen Wert.

Chancen und Risiken der weltweiten Vernetzung

Die Industrie 4.0 führt zu zunehmend digitalisierten und vernetzten Arbeits- und Fertigungsprozessen. Dabei fallen nicht nur zunehmend maschinengenerierte Daten an. Diese maschinengenerierten Daten werden zudem immer häufiger dezentral gespeichert und unternehmensübergreifend weiterverarbeitet. Der Austausch der Daten erfolgt dabei über Ländergrenzen hinweg.

Chancen

Der schnelle, weltweite Datentransfer ermöglicht ein effektiveres Arbeiten unabhängig vom Standort des Einzelnen.

So kann in einem Forschungs- und Entwicklungslabor in Kanada die Bauzeichnung für ein neues Produkt entwickelt und digitalisiert zentral abgespeichert werden.

Die gleiche Bauzeichnung kann in einem weiteren Fertigungsschritt in Deutschland abgerufen werden und ein 3D-Drucker fertigt aus der Bauzeichnung das Endprodukt an.

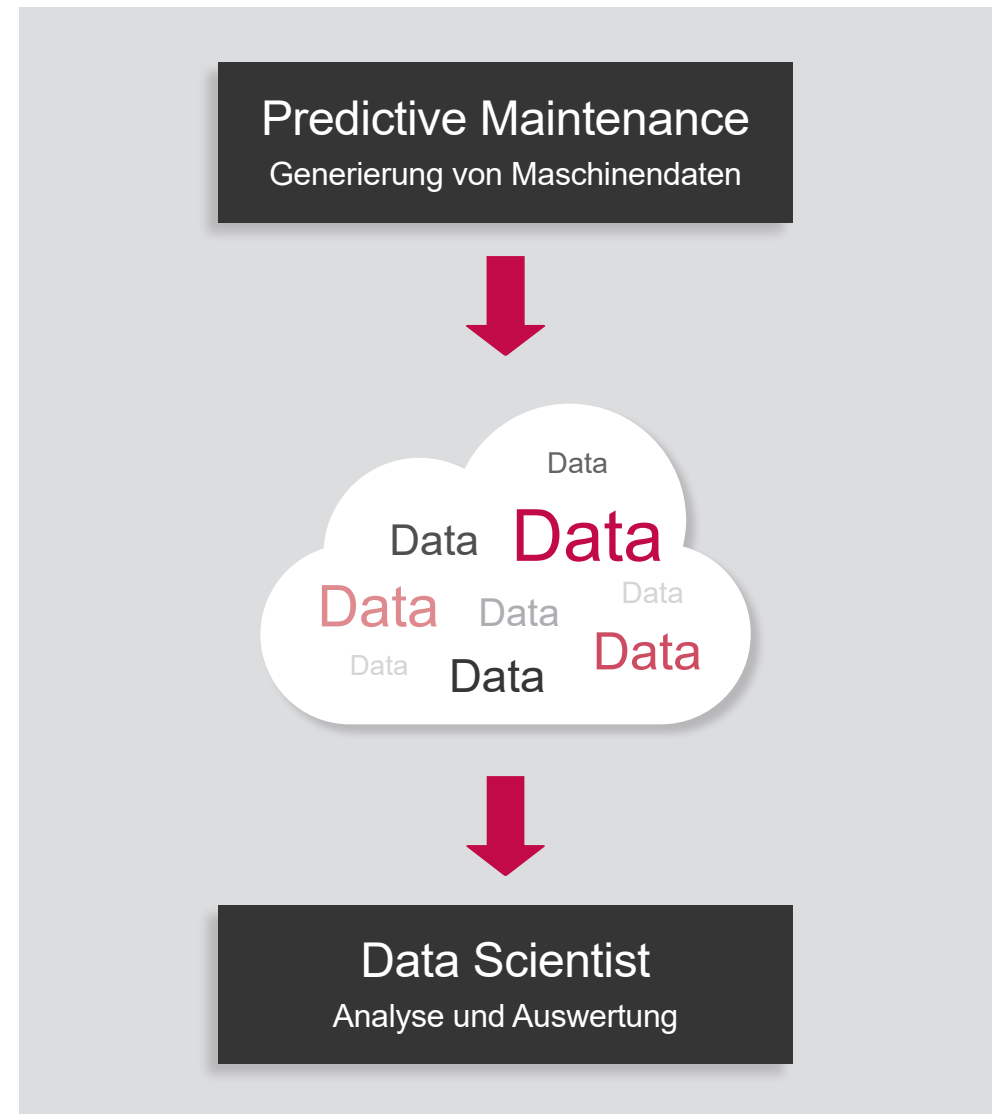
Risiken

Der weltweite Datenfluss hat selbstverständlich nicht nur Vorteile. Er birgt auch das Risiko, dass durch unsichere Kanäle auf das übermittelte Know-how von außen zugegriffen wird.

Digitalisierung: Entstehung neuer Fertigungsprozesse und Techniken

Auch werden beispielsweise im Rahmen von Predictive Maintenance zahlreiche Maschinendaten generiert. Diese werden dann dezentral in einer Cloud gespeichert, von wo aus ein Data Scientist zugreifen und diese zur weiteren Verwertung analysieren und auswerten kann. Diese Daten sind aber für das Unternehmen, welches gegenüber seinen Kunden die Predictive Maintenance Leistungen anbietet, von besonderer wirtschaftlicher Bedeutung.

Aber auch andere maschinengenerierte Daten, wie künftig die Smart Meter Daten, stellen Informationen dar, die für das erhebende Unternehmen wesentlich und damit schützenswert sind.



Mitarbeiter

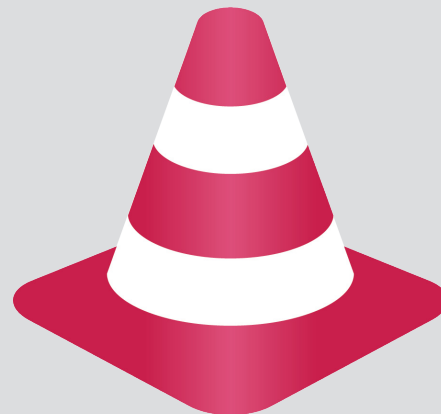
Der Schutz des eigenen, unternehmensinternen Wissens fängt in erster Linie bei den eigenen Mitarbeitern an. Diese müssen nicht nur für einen sorgsamem Umgang mit geheimen Informationen sensibilisiert werden.

Sie müssen auch über die Konsequenzen einer unberechtigten Weitergabe geheimer Informationen belehrt und insbesondere zur strikten Verschwiegenheit verpflichtet werden.

Das betrifft nicht zuletzt auch ausgeschiedene Mitarbeiter, die bewusst oder unbewusst ihrem alten Arbeitgeber schaden, in dem sie geheime Informationen zu ihrem neuen Arbeitgeber mitnehmen und diesem zur Verfügung stellen.

Die Abgrenzung zwischen (geschützten) Betriebs- und Geschäftsgeheimnissen und redlich erworbenen Erfahrungswerten/Kenntnissen eines Mitarbeiters bereitet hierbei erhebliche Schwierigkeiten, kann aber von entscheidender Bedeutung sein.

Risiko Faktoren



Kooperations-/Vertragspartner

Auch Kooperations- und Vertragspartner können für den Schutz von Know-how ein Risiko darstellen. Oftmals muss im Vorfeld einer Kooperation oder einer Finanzierung geheimes Wissen offenbart werden, damit der potentielle Kooperationspartner überprüfen kann, ob eine Zusammenarbeit mit dem eigenen Unternehmen überhaupt Sinn ergibt.

Die Preisgabe geheimer Informationen dient dann dazu, die eigene Expertise zu unterstreichen und zu belegen. Aber auch die bloße Machbarkeit einer geplanten Kooperation steht und fällt mit dem vorhandenen Know-how.

Im Gegenzug ist die direkte Einflussnahme auf den potentiellen Kooperationspartner äußerst gering. Auch die interne Organisation bzw. der interne Umgang mit geheimen Informationen ist außerhalb des eigenen Einflussbereichs, sodass auch Kooperationspartner einen nicht zu unterschätzenden Risikofaktor in Bezug auf das eigene Know-how darstellen.

Geschützt wurde Know-how in Deutschland bislang als Betriebs- bzw. Geschäftsgeheimnisse über das Wettbewerbsrecht (Geheimnisschutz). Dabei handelt es sich bei den wettbewerbsrechtlichen Vorschriften (§ 17 UWG) um Strafvorschriften, die den unberechtigten Abfluss von Know-how unter Strafe stellen.

Eine zivilrechtliche Zuordnung dieses Know-hows zu einem bestimmten Unternehmen als Inhaber, vergleichbar mit den gewerblichen Schutzrechten, wie Patent- oder Markenrechte, findet über den Geheimnisschutz jedoch nicht statt, sondern wird vielmehr vorausgesetzt.

Mit Umsetzung der Know-how-Richtlinie in das nationale Geschäftsgeheimnisgesetz (GeschGehG) erfährt der Know-how-Schutz in Deutschland eine wesentliche Reformierung.



Know-how-Richtlinie

Aufgrund der zunehmenden digitalen und grenzüberschreitenden Zusammenarbeit zwischen Unternehmen und der enormen wirtschaftlichen Bedeutung betrieblichen Know-hows hat sich die Europäische Union dazu entschieden, einen einheitlichen europäischen Geheimnisschutz zu schaffen.

Hierdurch soll ein einheitlicher europäischer Mindeststandard beim Schutz von Know-how geschaffen werden.

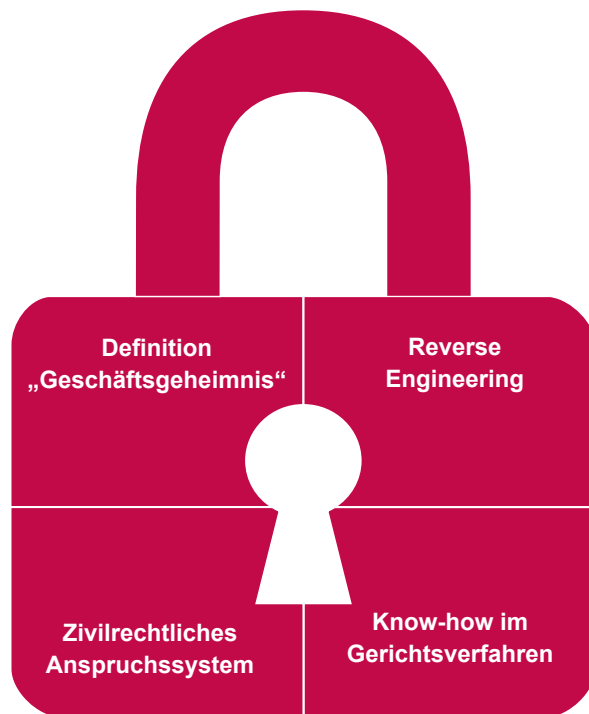
Mit der sogenannten **Know-how-Richtlinie**, die bis **Juni 2018** in nationales Recht umgesetzt werden musste, kommt es zu weitreichenden Veränderungen, die bereits jetzt zu einem Handeln der Unternehmen zwingen, wenn sie auch künftig ihr betriebliches Know-how geschützt wissen wollen.

Umsetzung der Know-how-Richtlinie

Seit dem **9. Juni 2018** gelten die neuen europäischen Vorgaben für den Geheimnisschutz, denn dies ist das Ablaufdatum der in der Know-how Richtlinie vorgegebenen Frist für die Umsetzung in nationales Recht. Ab diesem Stichtag sind deutsche Gerichte gehalten, das deutsche Recht zum Geheimnisschutz „europarechtskonform“ auszulegen.

Der Bundestag hat am 21.3.2019 über das GeschGehG abgestimmt, so dass die Know-how-Richtlinie nun auch in deutsches Recht umgesetzt wird.

Änderungen durch die Know-how-Richtlinie



Struktur von GeschGehG und Know-how-Richtlinie

Beim ersten Blick auf das GeschGehG wird die starke Richtlinienorientierung der deutschen Umsetzung deutlich. Sowohl das GeschGehG als auch die Richtlinie enthalten im jeweils ersten Abschnitt die allgemeinen Regelungen, nämlich die **Begriffsbestimmungen**, die **erlaubten Handlungen** (Richtlinie: rechtmäßiger Erwerb, Offenlegung und Nutzung von Geschäftsgeheimnissen), **Handlungsverbote** (Richtlinie: rechtswidriger Erwerb, Offenlegung und Nutzung) sowie die **Ausnahmetatbestände** (Richtlinie: „Ausnahmen“).

Es folgen in beiden Dokumenten im mittleren Teil die Regelungen zu den Ansprüchen bei Rechtsverletzungen sowie im letzten Drittel Bestimmungen zu Gerichts-, Prozess und Strafvorschriften.

Das GeschGehG enthält zudem einige Regelungen, die nicht unmittelbar aus der Richtlinie hervorgehen, die der nationale Gesetzgeber aber für die Integration der Richtlinienvorgaben in das deutsche Regelungsgefüge des Geheimnisschutzes für erforderlich hält.

Hierzu zählen der **Anspruch auf Auskunft**, die **Haftung des Inhabers eines Unternehmens** sowie **Regelungen zur Zuständigkeit der Gerichte** und eine **Härtefallregelung in der Streitwertbegünstigung**. Ähnliche Bestimmungen finden sich auch in anderen verwandten Gesetzen des gewerblichen Rechtsschutzes wie dem Marken- oder dem Patentgesetz.

Regelungen des GeschGehG im Einzelnen

Das „Geschäftsgeheimnis“ – Was ist geschützt?

Der Anwendungsbereich des GeschGehG ist eröffnet, wenn ein „Geschäftsgeheimnis“ im Sinne des § 2 Nr. 1 vorliegt. Hierunter versteht die gesetzliche Definition nach dem Entwurf eine Information,

- ▶ *a) die weder insgesamt 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 ist und daher von wirtschaftlichem Wert ist und*
- ▶ *b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und*
- ▶ *c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht“.*

Nach der Begründung soll diese Definition – wenn denn die vorgenannten qualitativen Voraussetzungen (Unbekanntheit, Wert, Maßnahmen) erfüllt sind – sowohl die bisher gebräuchlichen Begriffe des „Know-hows“ als auch des im deutschen Raum üblichen „Betriebsgeheimnisses“ umfassen. Bei solchen Informationen kann es sich also sowohl um technisches wie auch um kaufmännisches Wissen handeln.

Soweit als Voraussetzung die Unbekanntheit bzw. die Unzugänglichkeit der Information genannt wird, dient dies laut der Entwurfsbegründung dem Ausschluss von belanglosen Informationen sowie von Erfahrungen und Qualifikationen, die Beschäftigte im Zuge ihrer Anstellung erlangen sowie von Informationen, die generell bekannt oder leicht zugänglich sind.

Einen wirtschaftlichen Wert, der nach der Gesetzesformulierung („daher von wirtschaftlichem Wert“) gerade aus der Unbekanntheit bzw. Unzugänglichkeit resultieren muss, hat die Information, wenn sie Einfluss auf die Wettbewerbsposition hat und dem Inhaber bei Geheimhaltung einen Vorteil verspricht. Dies solle insbesondere auch den Schutz von Forschungsergebnissen von Universitäten ermöglichen, wenn diese am Wettbewerb teilnehmen. Dazu zählen sollen aber auch Herstellungsverfahren, Kunden- und Lieferantenlisten, Kosteninformationen, Geschäftsstrategien, Unternehmensdaten, Marktanalysen, Prototypen, Formeln und Rezepte. Nicht aber solche Informationen, bei denen zwar ein Geheimhaltungsinteresse des Inhabers besteht, dieser aber nicht am Wettbewerb teilnimmt.

In der qualitativen Voraussetzung der Schutzmaßnahmen liegt eine der zentralen Neuerungen des Geheimnisschutzrechts. Denn nach bisheriger deutscher Rechtslage genügte es, wenn eine geheime Tatsache von kommerziellem Wert nach dem erkennbaren subjektiven Willen des Inhabers geheim gehalten werden soll. Getreu dem Motto „handeln, nicht wünschen“ reicht also der bloße Wille des Informationsinhabers nicht mehr aus.

Hier ist in prozessualer Hinsicht zu beachten, dass dieses objektive Merkmal der vorgenommenen Maßnahmen dann auch im Streitfall vom Informationsinhaber zu beweisen ist. Beispiele für solche Maßnahmen sind physische Zugangsbeschränkungen und vertragliche Sicherungsmechanismen. Bedeutung erlangen hier insbesondere Geheimhaltungsvereinbarungen mit externen Vertragspartnern sowie – in bislang nicht bekannter Relevanz – vertraglich abzubildende Vertraulichkeits- und Geheimhaltungsvereinbarungen mit den eigenen Mitarbeitern. Auch eine nachvertragliche Schweigepflicht wird hierdurch noch stärker in den Fokus geraten.

Bedeutung erlangt auch das Kriterium der Angemessenheit. Denn die Information muss eben gerade nicht Gegenstand von „allen möglichen“ oder „zumutbaren“ Maßnahmen sein, sondern von „angemessenen“. Nach der Begründung bestimmt sich die Angemessenheit aus einer Abwägung zwischen dem Wert der zu schützenden Information, dessen Entwicklungskosten, seiner Bedeutung für das Unternehmen, die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen, die Art der Kennzeichnung der Information sowie etwaiger vorhandener vertraglicher Geheimhaltungsregeln.

Wie die Verbindung der Voraussetzungen durch „und“ verdeutlicht, müssen die genannten Voraussetzungen kumulativ vorliegen, es genügt also bspw. nicht, wenn die Information zwar am Markt unbekannt ist und daraus ihren Wert bezieht, jedoch durch das informationsinnehabende Unternehmen nicht Gegenstand bestimmter Schutzmaßnahmen gemacht wird.

§ 2 Nr. 2 und Nr. 3 GeschGehG enthalten darüber hinaus noch – im Vergleich zur Definition des Geschäftsgeheimnis – recht kurz gehaltene Definitionen dafür, wer Inhaber und wer Rechtsverletzer eines Geschäftsgeheimnisses ist. Nach dem GeschGehG ist dies die (natürliche oder juristische Person), die ein Geschäftsgeheimnis rechtmäßig erlangt hat und daher auch nutzen oder offenlegen darf bzw., im Falle des Rechtsverletzers, die Person, die rechtswidrig erlangt, nutzt und/oder offenlegt.

Als rechtsverletzende Produkte kommen nach § 7 Nr. 3 GeschGehG in Betracht: Produkte, deren Konzeptionen, Merkmale, Funktionsweisen, Herstellungsprozesse oder Marketing in erheblichem Umfang, soweit sie auf rechtswidrig erlangten, genutzten oder offengelegten Geschäftsgeheimnissen beruhen.

Erlaubte, verbotene und von Verboten ausgenommene Handlungen im Umgang mit Geschäftsgeheimnissen

Was im Hinblick auf Geschäftsgeheimnisse erlaubt, verboten oder ausnahmsweise von Verboten ausgenommen ist, bestimmen die §§ 3 – 5 GeschGehG. Dem entspricht die zugrundeliegende Richtlinie mit den Formulierungen „rechtmäßig, rechtswidrig“ und „Ausnahme“. Dabei geht das Gesetz grundsätzlich von der Handlungstrias „erlangen, nutzen, offenlegen“ als relevanten Aktionskreisen aus.

Erlaubte Handlungen

In § 3 GeschGehG sind die Fallgruppen geregelt, in denen die besagten Handlungen erlaubt sind. Anders als die Richtlinie verwendet das GeschGehG den Begriff der „Erlangung“ statt des „Erwerbs“, da über den rechtsgeschäftlichen Erwerb hinaus jegliche Kenntnisnahme eines Geschäftsgeheimnisses in dem Sinne erfasst werden soll, dass faktisch darüber verfügt werden kann. Dies beinhaltet entweder die aktive Kenntnisnahme des Geschäftsgeheimnisses oder bei in Gegenständen verkörperten Geschäftsgeheimnissen ein Ansichbringen des Gegenstands.

Zunächst enthält § 3 Abs. 1 GeschGehG die in Gesetzen übliche Erlaubnis für Handlungen durch Gesetz oder auf Grund eines Gesetzes. Aber auch die Erlangung, Nutzung oder Offenlegung durch Rechtsgeschäft sind naturgemäß erlaubt.

Interessanter, weil unklarer, sind die Erlaubnistatbestände des Abs. 2. Hiernach darf ein Geschäftsgeheimnis

„insbesondere erlangt werden durch

- ▶ *1. eine eigenständige Entdeckung oder Schöpfung;*
- ▶ *2. ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der*
 - a. öffentlich verfügbar gemacht wurde, oder*
 - b. sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt;*
- ▶ *3. ein Ausüben von Informations- und Anhörungsrechten der Arbeitnehmer oder Mitwirkungs- und Mitbestimmungsrechte der Arbeitnehmervertretung.“*

Das „insbesondere“ zu Beginn der Aufzählung dürfte so zu lesen sein, dass die danach aufgezählten Fallgruppen als Konkretisierung der gesetzlichen Erlaubnis (eben aufgrund des GeschGehG) zu verstehen sind. Nicht ausgeschlossen ist aber, dass dies eine Öffnungsklausel für bisher von der Rechtsprechung anerkannte oder zukünftig anzuerkennende, ungeschriebene Erlaubnissituationen darstellen soll.

Mit dem Schutz der eigenständigen Entdeckungen oder Schöpfungen soll verhindert werden, dass Exklusivrechte an Informationen begründet werden sollen, die als Geschäftsgeheimnisse geschützt sind; vielmehr soll es dem Umstand Rechnung tragen, dass es im Fall der parallelen Entdeckung oder Schöpfung mehrere Inhaber ein und desselben Geschäftsgeheimnisses geben kann.

Reverse Engineering

Nr. 2 legalisiert zukünftig das sog. „Reverse Engineering“, also die Entschlüsselung von Geschäftsgeheimnissen bzgl. Produkten aus den Produkten selbst. Auch hier liegt die bereits erwähnte Erwägung zugrunde, dass Exklusivrechte an Geschäftsgeheimnissen nicht begründet werden sollen. Nach der bisherigen Rechtslage war es so, dass nur dann ein zulässiges Reverse Engineering vorlag, wenn ein Fachmann ohne größeren Arbeits-, Zeit- und Kostenaufwand zur Ableitung in der Lage gewesen wäre.

Das Reverse Engineering wird aber auch zukünftig nicht grenzenlos erlaubt sein, sondern seine Beschränkungen in den immaterialgüterrechtlichen oder lauterkeitsrechtlichen Gesetzesschranken finden. Insbesondere bleibe beispielsweise die Herkunftstäuschung und Rufausbeutung nach § 4 Nr. 3 UWG unzulässig.

Nr. 2 lit. b) (rechtmäßiger Besitz und keine Erlangungsbeschränkung) gibt dem Geheimnisinhaber die Wahl, die Möglichkeit des Reverse Engineering vertraglich auszuschließen und so die Rechtmäßigkeit der Erlangung zu verhindern oder aber den Vertragspartner entsprechend gewähren zu lassen. Umgekehrt betrachtet bedarf es hier also einer aktiven Vertragsgestaltung durch den Geheimnisinhaber, wenn er das Reverse Engineering verhindern möchte.

In Nr. 3 ist klargestellt, dass die Ausübung der Mitwirkungs- und Mitbestimmungsrechte der Arbeitnehmervertretungen in Unternehmen sowie die Informations- und Anhörungsrechte der Arbeitnehmer grundsätzlich zu einer erlaubten Erlangung von Geschäftsgeheimnissen führen kann. Letztlich soll die derzeitige Rechtslage abgebildet werden, wonach Beteiligungsrechte der Arbeitnehmervertretungen nicht mit dem Hinweis auf das Vorliegen von Geschäftsgeheimnissen eingeschränkt werden dürfen. Arbeitsrechtliche Geheimhaltungsvereinbarungen bleiben hiervon unberührt.

Verbotene Handlungen

Eine der zentralen Vorschriften ist § 4 GeschGehG, welcher die in Bezug auf Geschäftsgeheimnisse verbotenen Handlungen regelt. Die Bedeutung dieser Norm folgt aus der Tatsache, dass Sanktionen in Gestalt der Ansprüche des verletzten Geheimnisinhabers (also Auskunft, Abfindung, Rückruf etc.) naturgemäß an einen Verstoß gegen ein Handlungsverbot geknüpft sind. Dabei ist § 4 GeschGehG stets zusammen mit § 5 GeschGehG zu prüfen, da dieser die Situationen regelt, in denen ein Verstoß gegen die Handlungsverbote ausnahmsweise nicht vorliegt.

Zielsetzung hinter § 4 GeschGehG ist nach der Begründung zu verhindern, dass Geschäftsgeheimnisse gänzlich der Gemeinfreiheit entzogen werden, was der Fall wäre, wenn dem Geheimnisinhaber ein Ausschließlichkeitsrecht gegenüber jedermann zugeordnet würde. Einer solch weitreichenden Wirkung soll die Festlegung eines Katalogs von verbotenen Handlungsweisen entgegenwirken, welcher den Geheimnisinhaber gerade nicht vor jeder zustimmungsfreien Handlung schützen soll, sondern eben nur vor den normierten.

Das GeschGehG regelt die Handlungsverbote – wieder unterteilt nach den drei Varianten „erlangen, nutzen, offenbaren“ – wie folgt:

- ▶ *„(1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch
 1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die sich im rechtmäßigen Besitz des Inhabers des Geschäftsgeheimnisses befinden und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
 2. jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.*

- ▶ *(2) Ein Geschäftsgeheimnis darf nicht nutzen oder offenlegen, wer
 1. das Geschäftsgeheimnis durch eine eigene Handlung nach Absatz 1
 - a) Nummer 1 oder
 - b) Nummer 2 erlangt hat,
 2. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt, oder
 3. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen.*

- ▶ *(3) Ein Geschäftsgeheimnis darf nicht erlangen, nutzen oder offenlegen, wer weiß oder wissen müsste, dass das Geschäftsgeheimnis entgegen Absatz 2 genutzt oder offengelegt worden ist. Das gilt insbesondere, wenn die Nutzung in der Herstellung, dem Anbieten, dem Inverkehrbringen, der Einfuhr, der Ausfuhr oder der Lagerung von rechtsverletzenden Produkten besteht.“*

Abs. 1 Nr. 1 des Verbotskatalogs zählt die verschiedenen verbotenen Handlungsarten sowie Handlungsobjekte auf. Das Abstellen auf das Unbefugtein verdeutlicht dabei, dass die Erlangung selbst zwar nicht unzulässig ist, wenn der Handelnde befugten Zugang zum Geschäftsgeheimnis hatte oder diese kopieren oder sich anderweitig aneignen durfte (bspw. weil er als Angestellter insofern Zugriff auf das Geschäftsgeheimnis hatte). Derartige „befugte“ Handlungen im Sinne des Abs. 1 Nr. 1 können jedoch unter Umständen dennoch die Voraussetzungen einer unzulässigen Nutzung oder Offenlegung nach Abs. 2 erfüllen.

Nr. 2 des ersten Absatzes stellt einen Auffangtatbestand dar und birgt als solcher bis zum Ergehen erster ober- und höchstrichterlicher Rechtsprechung erhebliche Rechtsunsicherheit für die Beteiligten, vor allem die potentiell zu Unrecht in Anspruch genommenen – vermeintlichen – Rechtsverletzer. Hier wird es in jedem Einzelfall auf die Interessenabwägung ankommen, wie sie sich in den Augen des erkennenden Gerichts darstellt. Als erste Abwägungskriterien nennt die Entwurfsbegründung dabei Handels- und Gewerbebräuche, verwerfliche Handlungen wie Vertrags- oder Vertrauensbruch sowie die Verleitung hierzu, aber auch den Grad des Verschuldens bzw. des Vorsatzes.

Der zweite Absatz normiert die Fälle, in denen eine Offenlegung verboten ist. Hervorzuheben ist Nr. 2 des Abs. 2, wonach die Nutzung bzw. Offenlegung trotz zunächst rechtmäßigen Zugangs – der nicht von Abs. 1 Nr. 1 erfasst ist, vgl. oben – verboten ist, wenn die das Geschäftsgeheimnis nutzende oder offenlegende Person gegen eine vertragliche oder sonstige Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt.

Beispiel ist hier insbesondere der Angestellte, der aufgrund seines Arbeitsverhältnisses zwar befugten Zugang zu einem Geschäftsgeheimnis erhält, allerdings ebenfalls aufgrund eben dieses Arbeitsverhältnisses zur Treue und Loyalität verpflichtet ist und daher eine Nutzung oder Offenbarung des zunächst rechtmäßig erlangten Geschäftsgeheimnisses verboten ist. In diesem Zusammenhang steht auch Nr. 3 des Abs. 2, wonach die Offenlegung ebenfalls unzulässig sein soll, wenn die das Geschäftsgeheimnis nutzende oder offenlegende Person gegen eine Vertraulichkeitsvereinbarung oder eine sonstige Verpflichtung verstößt. Wie hier letztlich eine Abgrenzung zu Nr. 2 erfolgt und welche (arbeits-)vertraglichen Gestaltungsvarianten in Frage kommen, wird die Rechtspraxis zeigen müssen. Laut Gesetzesbegründung soll aber unter den Begriff der Vertraulichkeitsvereinbarung auch die Verpflichtung von Arbeitnehmern im Arbeitsverhältnis zur Geheimhaltung und Loyalität fallen.

§ 4 Abs. 3 GeschGehG soll Situationen erfassen, in denen beispielsweise die Person, welche das Geschäftsgeheimnis erlangt hat, selbst keinen Verstoß im Sinne des Abs. 2 begangen hat, aber das Geheimnis von einem Dritten erhalten hat. In diesem Fall kommt es auf den Vorsatz bzw. die grob fahrlässige Unkenntnis dieser Person an.

Ausnahmen vom Anwendungsbereich

§ 5 GeschGehG sah in seiner ursprünglichen Fassung noch „Rechtfertigungsgründe“ vor. Nach zahlreicher Kritik verschiedener Verbände wurde § 5 GeschGehG neu gefasst. Nunmehr regelt er Bereichsmaßnahmen, wann das GeschGehG ausnahmsweise nicht zur Anwendung gelangt.

§ 5 enthält sodann eine nicht abschließende („insbesondere“) Aufzählung von Fällen, in denen der Anwendungsbereich des GeschGehG nicht eröffnet ist:

- ▶ 1. zur rechtmäßigen Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit nach der Charta der Grundrechte der Europäischen, einschließlich der Achtung der Freiheit und der Pluralität der Medien;
- ▶ 2. zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen;
- ▶ 3. im Rahmen der Offenlegung durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn dies erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann.“

Hinsichtlich Nr. 1 gilt es zu beachten, dass die EU-Charta in ihrer Gesamtheit einbezogen ist, also auch die in Art. 52 Abs. 3 Satz 1 enthaltene Einbeziehung von Art. 10 (Meinungsfreiheit) der Europäischen Menschenrechtskonvention. Hintergrund ist, dass für die Auslegung der Europäischen Menschenrechtskonvention der EGMR (Europäischer Gerichtshof für Menschenrechte) zuständig ist. Es ist daher nicht ausgeschlossen, dass über den Aspekt der „rechtmäßigen Ausübung des Rechts der freien Meinungsäußerung“ auch die EGMR Rechtsprechung für die Auslegung des § 5 Nr. 1 GeschGehG maßgeblich ist oder wird, wenn sich beispielsweise Arbeitnehmer als „Whistleblower“ auf ihre Meinungsfreiheit berufen.

§ 4 Nr. 2 GeschGehG dient explizit dem verstärkten Schutz der soeben bereits angesprochenen Whistleblower. Daher war diese Norm bislang auch häufigster Gegenstand der bislang vernehmbaren kritischen Stellungnahmen zum Entwurf des GeschGehG. Kritisiert wurde hier insbesondere die Tatsache, dass als Voraussetzung der Rechtfertigung die „Absicht“ geregelt wird, das öffentliche Interesse zu schützen, da dies die Fälle aus dem Anwendungsbereich fallen lasse, in denen der Whistleblower zwar nicht altruistisch handle, die Aufdeckung jedoch trotzdem im Interesse der Allgemeinheit stehe.

Als Beispiele für das in der Norm genannte „Fehlverhalten“ nennt die Entwurfsbegründung unethische Auslandsaktivitäten wie Kinderarbeit sowie auch gesundheitsschädliche oder umweltschädliche Produktionsbedingungen.

§ 5 Nr. 3 GeschGehG ergänzt schließlich den bereits in § 3 Nr. 3 erstrebten Arbeitnehmer- bzw. Arbeitnehmervertreterschutz. Laut Gesetzesbegründung privilegiert Nr. 3 aber die Nutzung oder Offenlegung von Geschäftsgeheimnissen im Rahmen der Offenlegung gegenüber Arbeitnehmervertretungen mit der Einschränkung, dass diese Offenlegung zur Aufgabenerfüllung der Arbeitnehmervertretung auch erforderlich war.

Ansprüche des Geschäftsgeheimnisinhabers bei Rechtsverletzungen

Jedes Verbot ist nur so wirksam wie die Sanktionen für einen entsprechenden Verstoß dagegen. Daher sieht das GeschGehG eine Reihe von Ansprüchen des Inhabers von Geschäftsgeheimnissen vor, die im Falle von Verstößen gegen Handlungsverbote gegen den Verletzer geltend gemacht werden können.

Zu diesen Ansprüchen zählen:

- ▶ der Anspruch auf Beseitigung und Unterlassung,
- ▶ der Anspruch auf Vernichtung, Herausgabe, Rückruf, Entfernung bzw. Rücknahme vom Markt, wobei die Herausgabe unter bestimmten Voraussetzungen auch noch nach Verjährungseintritt möglich ist,
- ▶ das Recht auf Auskunft über rechtsverletzende Produkte sowie auf Schadensersatz im Falle falscher oder nicht erfolgter Auskunft,
- ▶ der allgemeine Schadensersatzanspruch bei Verletzungen eines Geschäftsgeheimnisses
- ▶ sowie die Möglichkeit, einen etwaigen Anspruch unter bestimmten Voraussetzungen auch gegen den Inhaber eines Unternehmens zu richten, bei dem der Rechtsverletzer Beschäftigter ist.

Ihre Schranken finden diese Ansprüche insbesondere

- ▶ im Ausschluss der Ansprüche bei Unverhältnismäßigkeit,
- ▶ in der Möglichkeit des Rechtsverletzers, einen Anspruch nach dem GeschGehG durch Zahlung einer Geldabfindung abzuwenden
- ▶ sowie im allgemeinen Verbot der missbräuchlichen Geltendmachung der Ansprüche.

Strafbarkeit nach § 23 GeschGehG

Flankiert werden diese zivilrechtlichen Ansprüche von der Strafvorschrift des § 23, welcher dem Regelungsgehalt der bisherigen §§ 17 – 19 UWG entspricht, diese aber mit Blick auf die geänderten Marktverhältnisse modernisieren sowie an die Terminologie des restlichen GeschGehG anpassen soll.

Folglich entfällt hiernach die bisher getroffene Unterscheidung zwischen Betriebsgeheimnissen und Geschäftsgeheimnissen; fortan wird nur noch der Begriff des „Geschäftsgeheimnisses“ verwendet.

Neben den vorgenannten Motiven der Modernisierung und Harmonisierung soll ausdrücklich auch das sog. „Whistleblowing“ gestärkt werden, indem nämlich entsprechende Situationen vielfach aus dem Anwendungsbereich der Strafvorschrift herausfallen sollen.

Geschäftsgeheimnisse im Arbeitsverhältnis

Während des Arbeitsverhältnisses

Eine über bestehende Geheimhaltungspflichten (§ 79 BetrVG) hinausgehende Beschränkung ist durch das GeschGehG nicht vorgesehen, demnach sollte die derzeitige Rechtslage unverändert bleiben. Insbesondere sind die gewährleistete Tarifautonomie (§ 1 Abs. 3 Nr. 3) sowie die Betätigung der Arbeitnehmer und Betriebs- beziehungsweise Personalräte im Rahmen der betrieblichen Mitbestimmung von dem Anwendungsbereich des Gesetzes ausgenommen (§ 1 Abs. 3 Nr. 4, § 5 Nr. 3 GeschGehG).

Nach Beendigung des Arbeitsverhältnisses

Bisher unterlagen Arbeitnehmer nach Beendigung ihres Arbeitsverhältnisses auch ohne vertragliche Vereinbarung einer Verschwiegenheitspflicht hinsichtlich der Geschäfts- beziehungsweise Betriebsgeheimnisse. Um jedoch überhaupt in den Anwendungsbereich des Gesetzes zu gelangen, müssen die Informationen Gegenstand angemessener Geheimhaltungsmaßnahmen sein. Daher wird man nunmehr eine vertragliche Abrede als angemessene Geheimhaltungsmaßnahme des Arbeitgebers verlangen müssen, wenn man die Einstufung des entsprechenden Wissens als Geschäfts- oder Betriebsgeheimnis sichern will.

Praktische Überlegungen zu einem Schutzkonzept

Ein geeignetes Schutzkonzept muss technische und organisatorische Maßnahmen zum umfassenden Schutz von Geschäftsgeheimnissen gewährleisten können.

Das bedeutet z.B. auf technischer Seite, keinen ungeschützten Zugang zu vertraulichen oder kritischen Daten von nicht befugten Personen auf den Servern eines Unternehmensintranets. Ebenso müssen Personen auf arbeitsvertraglicher Ebene, die mit den geschützten Geschäftsgeheimnissen in Berührung kommen, durch Geheimhaltungsvereinbarungen und Wettbewerbsverbote an der Weitergabe von Geschäftsgeheimnissen gehindert werden.

Aufbau eines Schutzkonzepts

Der Aufbau eines solchen Schutzkonzepts erfolgt in verschiedenen Phasen.

Phase 1: Feststellungsphase

In einer Feststellungsphase muss überprüft werden, welche Informationen und welches Know-how im Unternehmen bestehen. Ferner sollte der Schutzbedarf des jeweiligen Geheimnisses aufgrund eines qualifizierenden Fragenkatalogs ermittelt werden. Ein solcher Fragenkatalog qualifiziert dann das jeweilige Geschäftsgeheimnis nach Vertraulichkeit und legt die Schutzstufe für das Geheimnis fest.

Phase 2: Planungsphase

Die Planungsphase bestimmt Maßnahmen, um bestehende und eventuelle Gefahren für den Verlust der in der vorherigen Feststellungsphase ermittelten Geschäftsgeheimnisse auszuschließen. Bei einer in der Planungsphase durchzuführenden Gefährdungsanalyse müssen dann Maßnahmen ausgewählt werden, die auf vertraglicher, technischer und organisatorischer Ebene garantieren, dass sich Gefahren zum Verlust von Geschäftsgeheimnissen nicht realisieren.

Phase 3: Umsetzungsphase

Die Umsetzung der vorher getroffenen Maßnahmen ist der wesentliche Bestandteil der Umsetzungsphase. Hier werden zahlreiche Abteilungen im Unternehmen an der Realisierung der jeweiligen Maßnahmen, beispielsweise der Verpflichtung zum Geheimnisschutz oder der Umsetzung von technischen und organisatorischen Maßnahmen beteiligt sein.

Phase 4: Prüfphase

Anschließend sollten die umgesetzten Maßnahmen auf ihre Wirksamkeit hin überprüft werden. Die Prüfphase zeigt hierbei im Rahmen von Audits sowie Erfahrungen den Verbesserungsbedarf am Geschäftsgeheimnisschutz auf und dient der Vorbereitung der Verbesserungsphase. Diese Phase dient insbesondere der Entdeckung von Schwachstellen, die entweder in der Vergangenheit zu einem Abfluss von Informationen geführt haben oder möglicherweise künftig führen können.

Phase 5: Verbesserungsphase

Innerhalb der Verbesserungsphase kann dann mittels einer Kosten-Nutzen-Analyse und auf Grundlage der Prüfphase stetig an dem Schutzkonzept gearbeitet werden.

Dr. Michael Rath

Rechtsanwalt
Fachanwalt für IT-Recht
Partner
Anna-Schneider-Steig 22
50678 Köln
Tel +49 221 9937 25795
michael.rath@luther-lawfirm.com

Dr. Maximilian Dorndorf

Rechtsanwalt
Partner
Gildehofstraße 1
45127 Essen
Tel +49 201 9220 24027
maximilian.dorndorf@
luther-lawfirm.com

Paul Schreiner

Rechtsanwalt
Fachanwalt für Arbeitsrecht
Partner
Gildehofstraße 1
45127 Essen
Tel +49 201 9220 11691
paul.schreiner@luther-lawfirm.com

Sebastian Laoutoumai, LL.M.

Rechtsanwalt
Fachanwalt für IT-Recht
Senior Associate
Gildehofstraße 1
45127 Essen
Tel +49 201 9220 24027
sebastian.laoutoumai@luther-lawfirm.com

Eine der führenden deutschen Anwaltskanzleien



Zahlen & Fakten

380 Rechtsanwälte und Steuerberater

10 Büros an zentralen deutschen Wirtschaftsstandorten

6 Büros an internationalen Finanzplätzen und Investitionsstandorten



Langjährige, enge Verbindungen zu renommierten Wirtschaftskanzleien weltweit



Regelmäßige Listung als führende und empfohlene Berater in den Fachmedien



LEADING INDIVIDUAL



Kanzlei des Jahres
für Energiewirtschaftsrecht



Kanzlei des Jahres
für Privates Baurecht



Kanzlei des Jahres
für Regulierte Industrien



Kanzlei des Jahres für
Vertrieb/Handel/Logistik



Kanzlei des Jahres für
Umwelt- und Planungsrecht

Luther.

Auf den Punkt. Luther.

