



# Das neue GeschGehG

Gesetz zum Schutz von Geschäftsgeheimnissen

Arbeitnehmer Parallelschöpfung Wettbewerb  
Alleinstellung Know-how Geschäftsgeheimnisse  
GeschGehG IT-Sicherheit Reverse Engineering  
Whistleblower Verschwiegenheit Urheberrecht  
angemessene Maßnahmen Unternehmenswert

## **Einleitung**

Nach den Änderungen im Datenschutzrecht durch die DSGVO wird auch das neue „Gesetz zum Schutz von Geschäftsgeheimnissen“ (kurz: GeschGehG) althergebrachte Handhabung von Abläufen in Unternehmen durcheinanderwirbeln. Das neue Gesetz wird derzeit vom Bundesministerium der Justiz als Umsetzung der Richtlinie 2016/943 vorbereitet und soll – planmäßig – am 01.01.2019 in Kraft treten. Allerdings endete der Umsetzungszeitraum der Richtlinie 2019/943 bereits am 09.06.2018, so dass deutsches Recht bis zum Inkrafttreten des GeschGehG bereits jetzt an den Anforderungen der Richtlinie zu messen ist.

Mit der Einführung der neuen gesetzlichen Regelungen beabsichtigt der Gesetzgeber ein Schutzkonzept zu etablieren, dass Know-how sowohl auf technischer als auch auf organisatorischer Ebene schützt. Dahinter steht die Erkenntnis, dass zur Entwicklung innovativer Produkte und Dienstleistungen in der Regel spezielles Know-how benötigt wird, welches man getrost auch als Herzstück eines jeden Unternehmens bezeichnen kann. Nicht immer stehen dem Unternehmen zum Schutz dieses Know-hows die klassischen „Registerrechte des geistigen Eigentums (Patente, Gebrauchsmuster, Marken, Designs) oder das Urheberrecht zur Seite.

Das neue Gesetz wird auch den Schutz von Geschäftsgeheimnissen vor Offenlegung im Rahmen eines gerichtlichen Verfahrens erheblich verbessern. So kann das Gericht zukünftig die Öffentlichkeit und den Kreis derjenigen, die Zugang zu den vollständigen Gerichtsakten und Schriftsätzen der Parteien erhalten, deutlich beschränken.

Schließlich sieht der Gesetzesentwurf auch Regelungen zum Schutz von Whistleblowern und Journalisten vor, indem es unter bestimmten Voraussetzung den Erwerb, die Nutzung oder die Offenlegung von Geschäftsgeheimnissen ausdrücklich erlaubt.

### **Was ist überhaupt ein „Geschäftsgeheimnis“?**

Eine der wesentlichsten Neuerungen des GeschGehG ist, dass der zentrale Begriff des Geschäftsgeheimnisses erstmals gesetzlich definiert wird. Im Grundsatz kann ein Geschäftsgeheimnis jegliche geschäftliche Information sein. Der Begriff umfasst Kundenlisten, Preislisten, Kalkulationsgrundlagen, Verfahrensweisen, Rezepturen, Muster, Prototypen, Konstruktionszeichnungen und -pläne, aber auch Markt- und Marketingstrategien.

Diese Informationen haben für Unternehmen eine erhebliche wirtschaftliche Bedeutung und können zu einem erheblichen Vorteil im Wettbewerb mit anderen Marktteilnehmern führen, sodass für den

Unternehmensinhaber ein hohes Interesse daran besteht, diese Informationen vor dem ungewollten Zugriff zu schützen.

Bisher definierte die Rechtsprechung unter einem Geschäftsgeheimnis jede im Zusammenhang mit dem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und die nach dem Willen des Betriebsinhabers aufgrund eines berechtigten Interesses geheim gehalten werden soll. Ein per Gesetz geschütztes Geschäftsgeheimnis lag bisher mithin schon dann vor, wenn ein Geheimhaltungswillen des Betriebsinhabers vorhanden war und dieser nach außen erkennbar war. Diese Erfordernisse ergaben sich nach der deutschen Rechtsprechung allerdings regelmäßig aus „der Natur der Sache“ oder „sien zu unterstellen“.

Hingegen sieht das GeschGehG zur Frage, ob geschäftliche Informationen zukünftig als Geschäftsgeheimnisse geschützt sind, eine Reihe äußerst praxisrelevanter Änderungen vor.

Nach § 1 Nr. 1 GeschGehG ein Geschäftsgeheimnis zukünftig nur dann vor, wenn

- es sich um eine der Allgemeinheit unbekannt Information handelt,
- die deswegen einen wirtschaftlichen Wert aufweist und
- die durch angemessene Geheimhaltungsmaßnahmen geschützt wird.

Das erste Merkmal dieser Definition, nach dem Informationen nur dann ein Geschäftsgeheimnis darstellen können, wenn 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, galt auch schon nach alter Rechtslage.

Neu ist, dass die Information von kommerziellem Wert für das Unternehmen sein muss, gerade weil sie geheim ist. Hierdurch sollen belanglose Informationen vom Schutz ausgeschlossen werden. Ob auch Informationen über rechtswidrige Vorgänge im Unternehmen hierunter fallen, die per se keinen wirtschaftlichen Wert haben, aber deren Bekanntwerden dem Unternehmen einen hohen Schaden zufügen würde, wird sich noch zeigen müssen.

Eine jedenfalls für die deutsche Praxis neue Schutzvoraussetzung ist, dass zur Begründung eines Geschäftsgeheimnisses zukünftig „angemessene Geheimhaltungsmaßnahmen“ getroffen werden müssen. Anderenfalls genießt die (ungeschützte) Information von vornherein nicht den Schutz des Gesetzes.

Schon vor 2000 Jahren legte Lucius Annaeus Seneca gewissermaßen den dahinterstehenden Grundsatz nieder: „Wenn du wünschst, dass ein anderer dein Geheimnis bewahre, dann bewahre es zuerst selbst“.

Ob ein geschütztes Geschäftsgeheimnis vorliegt, wird sich zukünftig also auch danach entscheiden, ob sich der Geheimhaltungswille des Betriebsinhabers in konkreten Schutzmaßnahmen manifestiert hat.

### **Was sind „angemessene Geheimhaltungsmaßnahmen“?**

Welche Arten von Geheimhaltungsmaßnahmen konkret erfolgen müssen, ist von der Art des Geschäftsgeheimnisses im Einzelnen abhängig. Grundsätzlich gilt, dass (nur) angemessene Maßnahmen, nicht aber alle „zumutbaren“ oder gar „möglichen“ Maßnahmen getroffen werden müssen. Schließlich hatte der Gesetzgeber insbesondere den Schutz von kleinen und mittelständischen Unternehmen im Blick, die er mit den neuen Vorschriften nicht über Gebühr belasten wollte.

Als Geheimhaltungsmaßnahmen kommen grundsätzlich sowohl physische Zugangsbeschränkungen wie auch vertragliche Sicherungsmechanismen (Vertraulichkeits- und Geheimhaltungsvereinbarungen mit externen Vertragspartnern und eigenen Mitarbeitern) in Betracht.

Bei der Wertung der Angemessenheit der Geheimhaltungsmaßnahmen können insbesondere berücksichtigt werden:

- ✓ der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten,
- ✓ die Bedeutung für das Unternehmen,
- ✓ die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen,
- ✓ die Art der Kennzeichnung der Information,
- ✓ die vereinbarten vertraglichen Regelungen mit Arbeitnehmern und Geschäftspartnern

Da das Erfordernis der „angemessenen Geheimhaltungsmaßnahmen“ sowohl auslegungsbedürftig als auch stark einzelfallabhängig ist, ist diese Frage von höchster Praxisrelevanz und wird zukünftig Gegenstand rechtlicher Auseinandersetzung sein.

### **Entwicklung eines Schutzkonzepts**

Um aktuell vorhandene und künftige Geschäftsgeheimnisse im Sinne des Gesetzes wirksam zu schützen, sollte für das Unternehmen ein Schutzkonzept entwickelt werden, das durch bestimmte festgeschriebene und umgesetzte Maßnahmen auf technischer und organisatorischer Ebene garantiert, dass Geschäftsgeheimnisse nach dem Gesetz begründet werden und sich der Verlust von Geschäftsgeheimnissen nicht verwirklicht. Hierfür bittet sich folgendes Vorgehen an:

Als erstes sollten die **Zuständigkeiten innerhalb des Unternehmens klar festgestellt werden**. Hierbei sollten insbesondere folgende Punkte Beachtung finden:

Sinnvoller Weise sollte je nach Größe des Unternehmens eine Person oder eine Gruppe von Personen fest mit der Verantwortlichkeit für den Geheimnisschutz beauftragt werden. So werden die Kompetenzen gebündelt und ist auch klar geregelt, wer Defizite zu verantworten und Lücken zu schließen hat.

Die Aufgabe des „Geheimnisbeauftragten“ ist eine Querschnittsaufgabe, die eine Koordination aller Fachabteilungen sowie die Schulung und Sensibilisierung von Mitarbeitern umfasst.

Sobald die Verantwortlichkeiten feststehen, ist als nächstes **potenziell geheimnis-relevantes Know-how des Unternehmens zu identifizieren**. Eine zugegebenermaßen aufwendige, jedoch absolut unverzichtbare Aufgabe, die in vielen Unternehmen auch zu zahlreichen „Aha-Erlebnissen“ führen wird.

Es empfiehlt sich ein Vorgehen entlang der Wertschöpfungskette:

- 1. Forschung und Entwicklung
- 2. Konstruktion und Fertigung
- 3. Marketing und Vertrieb
- 4. Kundenbetreuung

Anschließend ist eine **Bewertung und Kategorisierung des Know-hows** vorzunehmen. Häufiger Fehler dabei ist, dass unterschiedliche Interna undifferenziert zum „Geschäftsgeheimnis“ erklärt werden. Da das neue Gesetz zum Schutz von Geschäftsgeheimnissen jedoch angemessenen Schutzmaßnahmen zur Begründung eines Geheimnisschutzes verlangt, führt ein undifferenziertes Vorgehen an dieser Stelle zu einer Ausdünnung des Geheimnisschutzes. Im schlimmsten Fall können die betroffenen Informationen nicht mehr als Geschäftsgeheimnis im Sinne des Gesetzes angesehen werden. Wichtig

ist daher, das Know-how zu kategorisieren, um so den Umständen entsprechende „angemessene Maßnahmen“ definieren zu können.

Hierbei kann zwischen drei Qualitätsstufen unterschieden werden:

1. Echtes Schlüssel-Know-how
2. Strategisch besonders wichtiges Know-how
3. Sonstiges wettbewerbsrelevantes Know-how

Während der Verlust des sog. Schlüssel-Know-hows sich existenzgefährdend auswirken könnte, handelt es sich bei dem strategisch besonders wichtigem Know-how beispielsweise um Informationen bezüglich künftiger Technologiegenerationen, die sich noch im Vorstadium einer Schutzrechtsanmeldung befinden. Kostenintensive Schutzmaßnahmen sind vor allem in Bezug auf Gruppen 1 und 2 zu empfehlen. In der Regel fallen nur etwa 20% der „Betriebsgeheimnisse“ unter die ersten beiden Gruppen.

Ist das Know-How identifiziert und kategorisiert, sind dann die konkreten Schutzmaßnahmen festzulegen und umzusetzen. Hierzu zählen beispielsweise

- ✓ vertragliche Schutzmaßnahmen (Vertragsgestaltung im Verhältnis zu Geschäftspartnern, Dienstleistern und Mitarbeitern),
- ✓ technische Schutzmaßnahmen (Fragen der IT-Sicherheit, Zugangs- und Zutrittskontrolle, uva.) und
- ✓ organisatorische Maßnahmen (Arbeitsabläufe, Werks- und Gebäudeschutz).

Viele Maßnahmen sind parallel ohnehin im Rahmen der EU Datenschutzgrundverordnung (EU-DSGVO) umzusetzen, so dass es sich empfiehlt, die Schutzmaßnahmen mit dem Datenschutz abzustimmen.

### **Arbeitsrechtliche Gestaltungsmöglichkeiten**

Obwohl Wirtschaftsspionage durch Wettbewerber ein nicht zu unterschätzender Risikofaktor ist, sind in über 70 % der Fälle des Know-how-Abflusses die eigenen Arbeitnehmer beteiligt. Diese unterliegen zwar nach Beendigung des Arbeitsverhältnisses auch ohne ausdrückliche Vereinbarung der Verschwiegenheit über Geschäftsgeheimnisse. Allerdings darf der Arbeitnehmer gewonnene Erfahrungen zum eigenen Nutzen verwendet, solange er die Informationen aus seinem Gedächtnis

rekonstruieren kann. Fertigt sich der Arbeitnehmer während des Arbeitsverhältnisses jedoch Vermerke oder kopiert gar Dokumenten oder Daten und nutzt diese dann, verstößt er gegen seine arbeitsrechtliche Verschwiegenheitsverpflichtung.

In besagten Fällen des Know-how-Abflusses fehlt es den ausgeschiedenen Arbeitnehmern oft am Unrechtsbewusstsein für ihr Handeln, da ihnen das Bestehen oder die Reichweite ihrer Verschwiegenheitsverpflichtung nicht bewusst ist. Es empfiehlt sich für den Geschäftsgeheimnisinhaber eine ausdrückliche - schriftliche - Verschwiegenheitsverpflichtung mit seinen Arbeitnehmern zu vereinbaren. Hierbei muss insbesondere beachtet werden, dass eine Vereinbarung unwirksam ist, nach der Verschwiegenheit schlicht bezüglich sämtlicher unternehmerischer Belange zu wahren ist. Hier gilt es zu differenzieren.

Zum effektiven Schutz von Geschäftsgeheimnissen besteht auch weiterhin die Möglichkeit, eine nachvertragliche Wettbewerbsbeschränkung zu vereinbaren. Hierbei gelten allerdings enge gesetzliche Vorgaben, die beachtet werden müssen. Zur Sensibilisierung sollten Mitarbeiter zudem regelmäßig geschult werden.

### **Was tun bei Verletzungshandlungen?**

Wird ein Geschäftsgeheimnis rechtswidrig erlangt, benutzt oder offengelegt steht dem Inhaber ein bunter Strauß an Ansprüchen gegen den Rechtsverletzer zu. Zunächst kann der Inhaber des Geschäftsgeheimnisses vom Verletzer die Beseitigung und das Unterlassen der Beeinträchtigung verlangen. Hierfür ist nicht erforderlich, dass der Verletzer die Beeinträchtigung vorsätzlich oder fahrlässig herbeigeführt hat.

Ferner kann der Geschäftsgeheimnisinhaber den Rechtsverletzer auf Vernichtung oder Herausgabe der Dokumente und Gegenstände in Anspruch nehmen, die sich im Besitz oder im Eigentum des Rechtsverletzers befinden und die das Geschäftsgeheimnis enthalten oder dieses verkörpern. Geschäftsgeheimnisverletzende Produkte müssen zurückgerufen bzw. aus dem Markt entfernt werden.

Zur Abwendung dieser Ansprüche kann ein Rechtsverletzer, der weder vorsätzlich noch fahrlässig gehandelt hat, dem Inhaber des Geschäftsgeheimnisses eine Abfindung in Geld anbieten, wenn ihm durch die Erfüllung der Ansprüche ein unverhältnismäßig großer Aufwand entstehen würde und wenn eine Abfindung in Geld als angemessen erscheint. Die Höhe der Abfindung orientiert sich dabei an einer angemessenen Vergütung für die (fiktive) Einräumung entsprechender Nutzungsrechte.

Überdies hat der Gesetzgeber Ausschlussstatbestände für bestimmte Härtefälle geschaffen, in denen eine Erfüllung der Ansprüche durch den Rechtsverletzer unverhältnismäßig wäre. Im Einzelfall können Ansprüche des Geheimnisinhabers auf umfangreiche und kostspielige Rückrufmaßnahmen beispielsweise deshalb ausgeschlossen sein, weil das Geschäftsgeheimnis nur einen geringen Wert besitzt oder der Inhaber nur geringfügige Maßnahmen zum Schutz des Geschäftsgeheimnisses getroffen hat. Nach dem Gesetz sollen insbesondere das Verhalten des Rechtsverletzers, die Folgen der rechtswidrigen Nutzung, berechnete Interessen Dritter und das öffentliche Interesse (z.B. Whistleblower) bei der Frage der Verhältnismäßigkeit Berücksichtigung finden.

Selbstverständlich ist der vorsätzlich oder fahrlässig handelnde Rechtsverletzer zum Ersatz des dem Inhaber entstandenen Schadens verpflichtet – ohne dass er sich hierbei auf eine „Härtefallregelung“ berufen kann.

Neben diesen zivilrechtlichen Konsequenzen kann die rechtswidrige Erlangung, Nutzung oder Offenlegung auch strafrechtliche Konsequenzen (Freiheitsstrafe bis zu fünf Jahren) für den Rechtsverletzer haben. Die neue Strafvorschrift des § 22 GeschGehG entspricht im Wesentlichen den bisherigen Strafvorschriften des Gesetzes gegen den unlauteren Wettbewerb (§§ 17 bis 19 UWG), die lediglich den Begrifflichkeiten des Gesetzes zum Schutz von Geschäftsgeheimnissen angepasst worden ist.

### **Parallelschöpfung und Reverse Engineering**

Das neue Gesetz gewährt eigenständige (parallele) Entdeckungen oder Schöpfungen explizit den Schutz eines Geschäftsgeheimnisses. Dadurch soll verhindert werden, dass exklusive Rechte an Informationen begründet werden können. Somit ist es möglich, dass ein und dasselbe Geschäftsgeheimnis im Falle paralleler Entdeckungen oder Schöpfungen mehrere Inhaber hat.

Auch die Entschlüsselung von Geschäftsgeheimnissen aus den Produkten selbst, d.h. durch Beobachten, Untersuchen, Rückbauen und Testen eines Produkts (sog. Reverse Engineering) wird durch das neue Gesetz grundsätzlich erlaubt sein. Nach bisheriger Rechtslage war das Reverse Engineering nur zulässig, wenn ein Fachmann ohne größeren Arbeits-, Zeit- und Kostenaufwand zur Ableitung des Geschäftsgeheimnisses in der Lage war.

Beschränkungen bestehen lediglich dahingehend, dass das Produkt vom rechtmäßigen Besitzer öffentlich verfügbar gemacht wurde bzw. die untersuchende Person im rechtmäßigen Besitz des Produkts ist und kein Fall der Herkunftstäuschung oder Rufausbeutung vorliegt.



Ein Geschäftsgeheimnisinhaber der einem Vertragspartner untersagen möchte, das Know-how aus dem zur Verfügung gestellten Produkt abzuleiten, muss zukünftig explizite Vereinbarungen treffen.

### **Haftung des Inhabers des Unternehmens**

Das neue Gesetz sieht eine persönliche Haftung des Inhabers des Unternehmens vor, wenn das Geschäftsgeheimnis von einem Beschäftigten oder Beauftragten des Unternehmens rechtswidrig verletzt worden ist. Hintergrund ist, dass sich der Inhaber den Ansprüchen des Verletzten nicht mit dem Argument entziehen können soll, an der Rechtsverletzung selbst nicht beteiligt gewesen zu sein.

Die Verletzungshandlung des Beschäftigten bzw. des Beauftragen muss allerdings in einem unmittelbaren inneren Zusammenhang mit den von ihm wahrgenommen Aufgaben im Unternehmen stehen. Sofern der Verletzer im eigenen oder im Interesse Dritter handelt, ist eine persönliche Haftung des Inhabers ausgeschlossen. Die Haftung des Unternehmensinhabers schließt die (eigene) Haftung des Beschäftigten bzw. Beauftragten selbstverständlich nicht aus.

### **Schutz für Journalisten und Whistleblower**

Das neue Gesetz sieht auch einen verbesserten Schutz für Journalisten und sog. Whistleblower vor, wenn das Offenlegen der Geschäftsinformationen zum Schutz eines berechtigten Interesses erforderlich war. Ein berechtigtes Interesse soll insbesondere bei der rechtmäßigen Ausübung der freien Meinungsäußerung und der Informationsfreiheit vorliegen oder wenn das Verhalten zur Aufdeckung einer rechtswidrigen Handlung oder eines anderen Fehlverhaltens im Unternehmen dient.

Das Begriffspaar des „anderen Fehlverhaltens“ wirft dabei eine Menge Fragen auf, insbesondere da dieses Verhalten nicht gegen geltendes Recht verstoßen muss, um offengelegt werden zu dürfen. Der Europäische Gesetzgeber hatte hier offenbar Auslandstätigkeiten von Unternehmen im Blick, welche zwar in Europa, nicht aber im betreffenden Land einen Rechtsverstoß darstellen, z.B. Kinderarbeit, Steueroptimierung.

Damit ein Whistleblower keine zivil- und strafrechtlichen Konsequenzen fürchten muss, muss er jedoch auch in der Absicht handeln, das öffentliche Interesse zu schützen. Will er sich hingegen bei seinem alten Arbeitgeber rächen oder handelt er aus anderen rechtswidrigen Motiven, ist er in seinem Handeln nicht gerechtfertigt. In ihrem Umgang mit Whistleblowern sollten sich Unternehmen möglichst frühzeitig rechtssicher aufstellen, indem sie z.B. ein Hinweisgebersystem installieren und Führungskräfte und Arbeitnehmer geschult werden. Hierbei kommt dem Betriebsrat ein Mitbestimmungsrecht zu, weshalb sich der Abschluss einer Betriebsvereinbarung empfehlen kann.

## **Fazit: Handlungsbedarf**

Auch wenn das neue Gesetz zum Schutz von Geschäftsgeheimnissen bisher noch nicht in Kraft getreten ist, so finden die Regelungen der Europäischen Richtlinie bereits seit dem 09.06.2018 Anwendung. Es besteht damit bereits jetzt Handlungsbedarf, damit das Herzstück des Unternehmens – das Know-how – nicht verloren geht.

Technisch-organisatorische Geheimhaltungsregelungen sind zu definieren und umzusetzen, Vertraulichkeitsvereinbarungen sind zu aktualisieren bzw. neu zu gestalten. Verträge mit Vertragspartnern, Dienstleistern und Mitarbeitern, die mit dem Geschäftsgeheimnis in Berührung kommen, sind zu prüfen und gegebenenfalls zu ergänzen.

Insbesondere für Start-Ups ist ein sensibler Umgang mit dem vorhandenen Know-how sehr wichtig, da ein zu früh veröffentlichtes Geschäftskonzept die Gefahr birgt, dass betreffende Information nicht mehr als Geschäftsgeheimnis geschützt werden können und damit auch von Mitbewerbern verwendet werden können.



**Christian Koch**  
Rechtsanwalt  
Fachanwalt für  
Informationstechnologierecht  
Lehrbeauftragter der Technischen  
Hochschule Mittelhessen für IT-Recht



**Matthias Ache**  
Rechtsanwalt  
Rechtsanwalt mit Tätigkeitsschwerpunkt  
Gewerblicher Rechtsschutz  
Lehrbeauftragter der Technischen  
Hochschule Mittelhessen für  
Patentwesen

Kleymann, Karpenstein & Partner mbB  
Rechtsanwälte · Barrister · Notare  
Philosophenweg 1 · 35578 Wetzlar

[info@kleymann.com](mailto:info@kleymann.com)

T +49 (0) 6441 9446 – 0

F +49 (0) 6441 9446 – 46

[www.kleymann.com](http://www.kleymann.com)

[www.comcit.com](http://www.comcit.com)

Partnerschaftsgesellschaft mbB

AG Frankfurt/Main PR 1093

