

## Das neue Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

### Ein etwas zweifelhaftes Geschenk des Gesetzgebers

Schon im alten Troja musste man erfahren, dass Geschenke manchmal mit Vorsicht zu betrachten sind. Das neue Gesetz verspricht nun einen besseren Schutz der Geschäftsgeheimnisse zur Sicherung von Investitionen und Kapital der Unternehmen. Aber bei einem genaueren Blick merkt man, dass dieser Schutz nur dann eintreten kann, wenn man seine Geschäftsgeheimnisse mit einem nicht ganz unerheblichen Aufwand definiert, schützt und kontrolliert und das neue Gesetz liefert allen Whistleblowern in einem Unternehmen Schutz, wenn sie ihren Verrat nur geschickt begründen.

Beide Aspekte machen es notwendig, dass sich die Verantwortlichen in Unternehmen etwas ausführlicher mit diesem Gesetz, das ohne große öffentliche Aufmerksamkeit Ende April 2019 in Kraft getreten ist, genauer befassen und dabei überlegen, wie sie die notwendigen Schritte selbst oder mithilfe externer Experten rasch und zielführend, aber gleichwohl ohne unvermeidbaren finanziellen Aufwand durchführen können.

### Worum geht es nun im Einzelnen?

Das neue Gesetz formuliert bei der Verletzung von Geschäftsgeheimnissen klare Rechtsansprüche auf Beseitigung und Unterlassung. Der Rechtsverletzte kann auf Vernichtung oder Herausgabe der in seinem Besitz befindlichen Dokumente, Gegenstände, Materialien, Stoffe oder elektronischer Dateien, die das Geschäftsgeheimnis enthalten oder verkörpern, in Anspruch genommen werden. Rechtsverletzende Produkte sind zurückzurufen. Diese sind auch dauerhaft aus den Vertriebswegen des Rechtsverletzers zu entfernen und schließlich insgesamt zu vernichten. Dem Inhaber der Rechte stehen Auskunftsansprüche zu. Der Rechtsverletzer hat schließlich dem Inhaber des Geschäftsgeheimnisses Schadensersatz zu leisten. Bei der Bemessung des Schadenersatzes kann sogar der Gewinn, den der Rechtsverletzer erzielt hat, berücksichtigt werden. Das klingt alles sehr schön und ist es auch und stellt sicherlich in vielerlei Hinsicht eine Vereinfachung zur bisherigen Rechtslage dar. Wo also ist der Haken?

Nun, es geht doch zunächst schlicht um die Frage, was ist ein Geschäftsgeheimnis und immerhin, das Gesetz definiert diesen Begriff nun in § 2. Geschäftsgeheimnisse sind Informationen und zwar solche, die nicht allgemein bekannt und ohne weiteres zugänglich sind und daher einen wirtschaftlichen Wert darstellen.

Soweit so gut, aber das Gesetz stellt weitere Erfordernisse auf, um ein schützenswertes Geschäftsgeheimnis anzuerkennen. Die Information muss nämlich durch nach den Umständen angemessene Geheimhaltungsmaßnahmen geschützt sein.

Zusätzlich muss der Inhaber ein berechtigtes Interesse an der Geheimhaltung haben. Der Begriff „angemessene Geheimhaltungsmaßnahme“ und der Begriff „berechtigtes Interesse an der Geheimhaltung“ ist dabei nicht weiter gesetzlich definiert.

Wir haben also zwei unbestimmte Rechtsbegriffe, die durch die Rechtsanwender, letztlich durch die Gerichte, auszulegen sind. Inhaber des Geheimnisses kann dabei jede natürliche oder juristische Person sein, die in der Lage ist, eine rechtmäßige Kontrolle über ein Geschäftsgeheimnis auszuüben. Was genau hier wieder „Kontrolle“ heißt, bleibt ebenfalls offen.

Es werden nur solche Informationen geschützt, für die angemessene Geheimhaltungsmaßnahmen bestehen, die ihrerseits einer rechtmäßigen Kontrolle durch den Inhaber unterliegen, der wiederum ein berechtigtes Interesse an der Geheimhaltung haben muss. Viele Fragen also für die praktische Anwendung dieses neuen Gesetzes und es verwundert nicht, dass man schon heute voller Neugier und Interesse auf die ersten gerichtlichen Entscheidungen hierzu wartet.

## Welche Maßnahmen sollten getroffen werden?

Schnell schwirrten viele Angebote von mehr oder weniger großen Experten durch das Land in denen oft für teures Geld ein Schutz angeboten wurde, der vielleicht noch versuchte, die juristischen Probleme zu lösen, aber kaum je hilfreich war, die technische Seite des Schutzes und der Kontrolle aufzugreifen. Wer weiß, dass er schützenswerte Geschäftsgeheimnisse hat, der sollte wohl eher auf Nummer sichergehen, denn sowohl die Geheimhaltungsmaßnahmen, als auch ihre Kontrolle müssen im Zweifel „gerichtsfest“ sein.

Die Erstellung eines Schutzkonzepts und die Umsetzung der notwendigen und angemessenen Maßnahmen stellt Unternehmen vor eine schwierige Herausforderung. Kein anderes Gesetz erfordert derart wirtschaftliches, technisches und rechtliches Schnittstellenwissen. Nur Unternehmen, die sich dem Kern ihres Erfolges, ihrem Wissen positiv stellen, werden in der Zukunft die Konsequenzen, die sich aus dem neuen Gesetz ergeben, erfolgreich meistern und ohne Schaden bleiben.

Reichen vielleicht doch klar gefasste pauschalierte Erklärungen in den Verträgen mit Geschäftspartnern und Mitarbeitern als wirksamer Schutz aus? Definitiv reicht das als Schutzmaßnahme nicht! Wir fürchten, dass das neue Gesetz eine Systemänderung bedeutet und, dass der Inhaber des Geschäftsgeheimnisses einer hohen Beweislast unterliegt.

Man tut sich aktuell noch schwer, alle Aspekte des Gesetzes zu berücksichtigen, doch zeigen Angebote moderner Technologieunternehmen, dass man sowohl bei der Erstellung von Schutzkonzepten, als auch bei deren Umsetzung einen hohen Automatisierungsgrad einsetzten können, der zudem einen branchenunabhängigen, raschen und letztlich kosteneffizienten Schutz der Geschäftsgeheimnisse bieten kann.

Durch die hohe Nachweisdichte der Technologie könnten hier wohl relativ sicher die notwendigen, weil belastbaren Beweislagen geschaffen werden um Geschäftsgeheimnisse zu definieren, zu schützen und den Schutz zu kontrollieren.

Die Technologie dieser Schutz- und Kontrollmethode scheint uns derzeit auch das einzige wirksame Instrument zu sein, um die Geheimnisse auch international und sprachunabhängig schützen zu können.

In einer Reihe von Gesprächen konnte dabei auch die Vorstellung entwickelt und bestätigt werden, diese Technologien synchron für die Erfordernisse des Datenschutzes zu nutzen.

Man merkt hier aber gerade als Jurist sofort, wie schnell man bei der Beschreibung der Konsequenzen dieses Gesetzes und der Schaffung der notwendigen Vorkehrungen den rein rechtlichen Rahmen verlässt und zu einer technologischen und wirtschaftlichen Gesamtbetrachtung kommen muss.

## Was ist ein Geschäftsgeheimnis?

Geschäftsgeheimnis ist nur das, wofür es ein berechtigtes Interesse gibt.

Und damit kommen wir schon zu dem Problem der Hinweisgeber. Während § 4 des Gesetzes noch die Handlungsverbote beschreibt, wie man nämlich ein Geschäftsgeheimnis nicht erlangen darf und warum man ein solches auch nicht nutzen darf, schafft § 5 mehrere schwerwiegende Ausnahmen. Die Erlangung, Nutzung oder Offenlegung eines Geschäftsgeheimnisses ist nicht verboten, wenn diese Handlungen zum Schutze eines berechtigten Interesses erfolgen. Das Gesetz zählt hier 3 Beispiele auf:

- Die Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit, einschließlich der Achtung der Freiheit und der Pluralität der Medien
- Zwecke der Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen und schließlich
- Verletzungshandlungen im Rahmen der Offenlegung durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn dies erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann.

Vor Inkrafttreten des Gesetzes war es einem Mitarbeiter klar verboten, Geschäftsgeheimnisse nach außen zu geben und er konnte sich nach den Strafbestimmungen des UWG auch strafbar machen. Wer zu einer derartigen Handlung auffordert, machte sich, wenn dies öffentlich geschah, gleichfalls strafbar nach § 111 StGB. Es gab aber jetzt, schon gleich nach dem Inkrafttreten des Gesetzes, die ersten Urteile, die ohne große Umschweife erklären, wer in einem Unternehmen Fragwürdiges tue, könne sich eben nicht auf den Schutz von Geschäftsgeheimnissen berufen. Unter sonstigen Fehlverhalten fielen dabei alle Dinge, die zwar rechtlich erlaubt, aber ethisch irgendwie fragwürdig sind.

## Schutz vor Whistleblowern

Ist man hier hilflos jeder Form einer, eventuell auch nur vorgeblichen, Gesinnungsethik ausgeliefert? Kann man sich dann, wenn der Geheimnisverrat unter diesem Vorwand erfolgt, auch nicht mehr gegen derartig getarnte aber gezielte Angriffe von Mitbewerbern wehren?

Allein rechtlich wird dies schwierig sein, aber es sollte möglich sein, durch den Einsatz der bereits oben erwähnten Technologien schnell und leicht zu erkennen, wo und wie der Informationsfluss zu und von Hinweisgebern im Unternehmen verläuft. Kann man nachweisen, dass Informationen nicht nur an die Medien gegeben wurden um auf einen himmelschreienden Unrechtsvorgang hinzuweisen, sondern auch, dass diese Aktion lange und unter Beteiligung wirtschaftlich interessierter Dritte vorbereitet war, kann es vielleicht gelingen Staatsanwaltschaften und Gerichte davon zu überzeugen, dass die Verletzung von Informationen hier nicht geeignet war, das allgemeine öffentliche Interesse zu schützen, sondern ganz andere Ziele und Zwecke verfolgte.

Stark vereinfacht funktioniert die angesprochene Technologie dergestalt, dass nach der betriebsspezifischen Definition des Geschäftsgeheimnisses beschrieben wird, wer Zugang zu welchen Geschäftsgeheimnissen haben darf und wer an wen und mit wem zulässig Informationen hierüber geben bzw. austauschen darf. Basierend auf diesen Parametern erstellt man eine Wissensinventur für das gesamte Unternehmen oder, falls das Unternehmen zu groß ist, auch für seine Teilbereiche. Zunächst wird damit nur der Istzustand festgestellt.

Schon hieraus sieht man aber oft Schwachstellen und erkennt, welcher Handlungsbedarf für Schutzmaßnahmen noch besteht. Die Technologie erfasst ab Implementierung aber auch alle Veränderungen. Alle Regelwidrigkeiten, aber auch alle regelkonformen Anhäufungen von Geschäftsgeheimnissen oder ein plötzlicher Abfluss der Informationen, lassen sich im Zeitraffer leicht erkennen und auf ihre Ursachen hin hinterfragen. Die Abbildung des Ablaufs von Informationserhalt, - Besitz und - Weitergabe in der Zeitdarstellung liefert schnell und automatisiert Hinweise auf regelwidrige Abweichungen insbesondere bei Abgleich mit relevanten Ereigniszeitpunkten. Der Analyse-Algorithmus kann dabei unternehmensspezifisch gestaltet werden. Gibt das System Alarm, dann ist durch die verantwortliche Stelle zu entscheiden, wie und mit welchen Maßnahmen unter Beachtung der Datenschutzrechte eine Erklärung für den automatisierten Warnruf zu veranlassen ist.

Was eingangs vielleicht noch als übertrieben erschien, nämlich, dass es hier um wichtige Schnittstellen von wirtschaftlichem Wissen, rechtlichen Gegebenheiten und dem Einsatz von Technologien geht um ein Unternehmen wirksam zu schützen, erscheint jetzt vielleicht etwas plausibler.

## Fazit und Empfehlungen

Das neue Gesetz, das letztlich auf einer europäischen Richtlinie fußt, ist kein Gesetz für die Unternehmen geworden. Es stellt diese vielmehr vor neue und schwierige Herausforderungen.

Denken Sie bitte auch daran, dass die Richtlinie in ihren wesentlichen Eckpunkten in allen Ländern der EU gilt und insoweit Tochterunternehmen, außerhalb Deutschlands, diesen Umstand unbedingt auch berücksichtigen müssen.

Hält man sich dies vor Augen, dann erscheint der Vergleich des GeschGehG mit dem Danaergeschenk des Trojanischen Pferdes vielleicht gar nicht mehr so schief. Was aber kann ich als Anwalt einem Unternehmen raten, um das „Gesetzesgeschenk“ nicht nur zur Gefahr werden zu lassen?

Einige Aspekte aus den nachfolgenden Stichpunkten sollte daher jedes Unternehmen bedenken, um nicht völlig ohne Beweismittel nur noch resigniert die Segel streichen zu müssen:

- Beschreiben Sie ein Projekt hinsichtlich seines Umfangs und Inhalts zur rechtskonformen Umsetzung des neuen Gesetzes.
- Klassifizieren Sie Ihre Geschäftsgeheimnisse entsprechend den neuen Begriffsbestimmungen.
- Entwickeln Sie einen Maßnahmenkatalog für die Umsetzung als Schutzkonzept.
- Fertigen Sie Prüfberichte über die tatsächliche Umsetzung der Schutzmaßnahmen.
- Dokumentieren Sie, wer Insiderwissen über kaufmännische oder technische Informationen aus oder über Ihr Unternehmen hat. Stellen Sie sicher, dass auch Änderungen des Personenkreises stets erfasst werden. Denken Sie bitte auch daran, dass auch externe Berater häufig über Insiderwissen verfügen. Lassen Sie sich von diesen stets zusichern, dass alle von Ihnen erlangten Informationen vertraulich behandelt werden und verlangen Sie, dass hierüber gegebenenfalls ein Nachweis erbracht werden muss.
- Fertigen Sie Protokolle über sämtliche Vertragsanpassungen mit internen und externen Trägern von Geschäftsgeheimnisträgern.
- Sichern Sie stets weiteres zweckbestimmtes Beweismaterial.
- Denken Sie auch an die Sicherung des Materials für Mitarbeiterschulungen.
- Wenn Sie eine zeitgemäße Kontrolle Ihrer in digitaler Form vorhandenen Geschäftsgeheimnisse planen, dann sollten Sie hierfür auch ein automatisiertes Warnsystem mit vorsehen. Dieses erfasst alle Datenbewegungen. Informationsflüsse in einem Unternehmen zeigen stets eine große Kontinuität im laufenden Geschäftsbetrieb.

Alle Abweichungen hiervon sind Signale, die Sie veranlassen sollten, diese Auffälligkeiten sorgfältig zu analysieren. Natürlich wird bei einem neuen Projekt oder anderen geplanten bzw. bekannten Besonderheiten hierfür ein erhöhter Datenaustausch anfallen. Das ist aber schnell als gewollte und notwendige Abweichung erkannt. Aber häufig verschwinden Daten ja auch schleichend. Hier hilft die Möglichkeit, dass das System aufgrund seiner Algorithmen auch Untersuchungen im Zeitraffer vornimmt. Nach den Erfahrungen aus dem Sicherheitssystem von Banken und Finanzinstituten lassen sich so relativ rasch Quellen und Ursachen von Informationsverlusten finden.

---

## WHITE PAPER

Eine Information von DIE FAMILIENUNTERNEHMER e. V.  
Kommission Wettbewerb- und Wirtschaftsrecht

Juli 2019 | Hans-Peter Huber  
Tsambikakis & Partner Rechtsanwälte mbB | Berlin