Betriebs- und Geschäftsgeheimnisse 4.0
GeschGehG und der „digitale Safe“ – Unternehmen sind gefordert!

EINFÜHRUNG

Jeder kennt es, denn regelmäßig, wenn sog. „Know-How-Träger“ aus Sales, Entwicklung oder ähnlichen sensiblen Bereichen zur Konkurrenz wechseln oder sogar Target gezielter Abwerbemaßnahmen geworden sind, geht es nicht nur um „Köpfe“, sondern auch um das gegenständliche Know-How, mit dem die genannten Personen zwangsläufig in Kontakt gekommen sind. Egal ob bestimmte Bau- und Konstruktionspläne, Fertigungsverfahren, Rezepturen, Marketingstrategien, Montageanleitungen oder die profane Kundenliste, dem Schutz von Betriebs- und Geschäftsgeheimnissen kommt gerade im schnelllebigen Zeitalter von Globalisierung, Digitalisierung und Arbeiten 4.0 eine immer wichtigere Bedeutung zu.

Dies dürfte nunmehr auch den Gesetzgeber dazu bewogen haben, das Betriebs- und Geschäftsgeheimnis aus seinem gesetzlichen Schattendasein in § 17 UWG zu befreien und ein ganzheitliches Gesetz zum Schutz von Betriebs- und Geschäftsheimnissen auf den Weg zu bringen *(GeschGehG)*. Soweit die positive Nachricht, die negative – jedenfalls aus Unternehmenssicht – folgt auf dem Fuße. Denn eines der zentralen Elemente des *GeschGehG* ist eine gesetzliche Definition des Geheimnisbegriffs selbst, die den Unternehmen – anders als in der Vergangenheit – schon im Vorfeld einige Maßnahmen abverlangt, um für den Ernstfall gewappnet zu sein und den rechtlichen Schutz von Betriebs- und Geschäftsgeheimnissen nicht zu verlieren.

VEROBJEKTIVIERTER GEHEIMNISBEGRIFF: ANGEMESSENE MASSNAHMEN

Eines der Kernaspekte des Ende März 2019 durch den Bundestag verabschiedeten und im April jüngst auch durch den Bundesrat gebilligten „Gesetzes zum Schutz von Betriebs- und Geschäftsgeheimnissen“ *(GeschGehG)* ist der verobjektivierte Geheimnisbegriff. Während nach § 17 UWG im Wesentlichen ein subjektiver Geheimhaltungswille (der sich objektiv lediglich in irgendeiner Form manifestieren musste) ausreichte, wird nach § 2 Abs. 2 GeschGehG folgendes eingefordert:

Geschäftsgeheimnis ist (nur) eine Information, die

a) *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) *Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist.*

Zentral in diesem Zusammenhang ist das Erfordernis **angemessener Geheimhaltungsmaßnahmen**, über deren konkrete Form auch der Gesetzgeber jedenfalls einige Grundsätze an die Hand gibt (vgl. BT-Drucks. 18/4724, S.24f.):

*„Welche Arten von Geheimhaltungsmaßnahmen konkret erfolgen müssen, hängt von der Art des Geschäftsgeheimnisses im Einzelnen und den konkreten Umständen der Nutzung ab. In Betracht kommen sowohl **physische Zugangsbeschränkungen** und Vorkehrungen wie auch **vertragliche Sicherungsmechanismen**. Es ist nicht erforderlich, jede geheim zu haltende Information gesondert zu kennzeichnen, sondern es können grundsätzlich Maßnahmen für bestimmte Kategorien von Informationen ergriffen werden (zum Beispiel technische Zugangshürden) oder durch allgemeine interne Richtlinien und Anweisungen oder auch in Arbeitsverträgen vorgegeben werden.*

Bei der Wertung der Angemessenheit der Schutzmaßnahmen können insbesondere berücksichtigt werden: der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten, die Natur der Informationen, 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.“

WEITERE ELEMENTE: WHISTLEBLOWERSCHUTZ ETC.

Neben diesem neuen Geheimnisbegriff gibt es auch weitere Neuerungen, die den Geheimnisschutz in der Tendenz schwächen dürften. Hierzu gilt vor allem ein sog. **Schutz von Whistleblowern,** wonach eine Offenlegung von Geschäftsgeheimnissen u.a. dann gerechtfertigt sein soll, wenn dies zum Schutz eines berechtigten Interesses erfolgt.

PRAXISHINWEIS: „DIGITALER SAFE“ ERFORDERLICH

Das *GeschGehG* als Reformatio in peius? Wohl ja, aber völlig unabhängig davon, wie man zu den gesetzlichen Neuerungen steht, **Unternehmen sind nunmehr gefordert!** Bislang musste nahezu nichts getan werden, um rechtlichen Schutz für Betriebs- und Geschäftsgeheimnisse in Anspruch zu nehmen, Bestandsschutz

gab es nahezu automatisch. Das ändert sich jetzt. Bereits **im Vorfeld ist ein umfassendes Schutzkonzept** notwendig, um sich im Ernstfall wehren zu können, und zwar auf drei Ebenen:

(i) **Rechtliche Ebene**: Hierzu gehören vor allem Geheimhaltungsvereinbarungen bzw. -hinweise auf allen Ebenen, u.a. auch in Arbeitsverträgen bzw. internen Richtlinien/Weisungen, aber auch in weiteren Werk-/Dienstverträgen mit externen Kooperationspartnern und Dienstleistern.

(ii) **Organisatorische Ebene:** Zudem sind organisatorische Maßnahmen wie bspw. Zugangsbeschränkungen erforderlich, um sicherzustellen, dass der Personenkreis auf die Geheimhaltungsträger beschränkt bleibt, für deren Tätigkeit die Informationen notwendig sind.

(iii) **Technische Ebene:** Schließlich kommen im Zeitalter von Digitalisierung auch IT-Sicherheitsmaßnahmen eine wesentliche Bedeutung zu, soweit Geschäftsgeheimnisse – wie nahezu immer – in digitaler Form vorhanden sind.

Fehlt es an derartigen Maßnahmen, werden sich Unternehmen kaum noch auf ein Geschäftsgeheimnis berufen können. **Arbeitsrechtliche Sanktionen aller Art, Unterlassungs-, Schadensersatz- und/oder Vertragsstrafen laufen dann ins Leere!**

Deshalb ist dringend zu empfehlen, den gegenwärtigen Stand der Schutzmaßnahmen zu beleuchten. Auch dies wird in der Regel **kein „Hexenwerk“** sein, denn trotz des weiten Geheimnisbegriffs des UWG haben Unternehmen in der Praxis allein aus tatsächlichen Schutzerwägungen bereits oftmals eine Vielzahl der genannten Maßnahmen getroffen, sodass es lediglich die ein oder andere **Stellschraube in den (Arbeits-) Verträgen, internen Richtlinien etc.** an die neuen Anforderungen anzupassen gilt. Gleichwohl sollte dies zügig angepackt werden, um den rechtlichen Bestandsschutz von Betriebs- und Geschäftsgeheimnissen nicht zu verlieren!

Zögern Sie bitte nicht, uns bei Fragen zu diesem Thema anzusprechen. Gerne nehmen wir Sie – soweit noch nicht geschehen – auch auf den Verteiler unseres kostenlosen Kanzlei-Newsletters auf, in dem wir regelmäßig auch arbeitsrechtliche Fragen sowie Fragen an der Schnittstelle zu Compliance (IVV, Datenschutz, AÜG, Investigations etc.) behandeln. Schicken Sie uns zu diesem Zweck gerne einfach eine kurze **Mail**.

KONTAKT

Dr. Thilo Mahnhold
t.mahnhold@justem.de

Dr. Daniel Klösel
d.kloesel@justem.de

www.justem.de