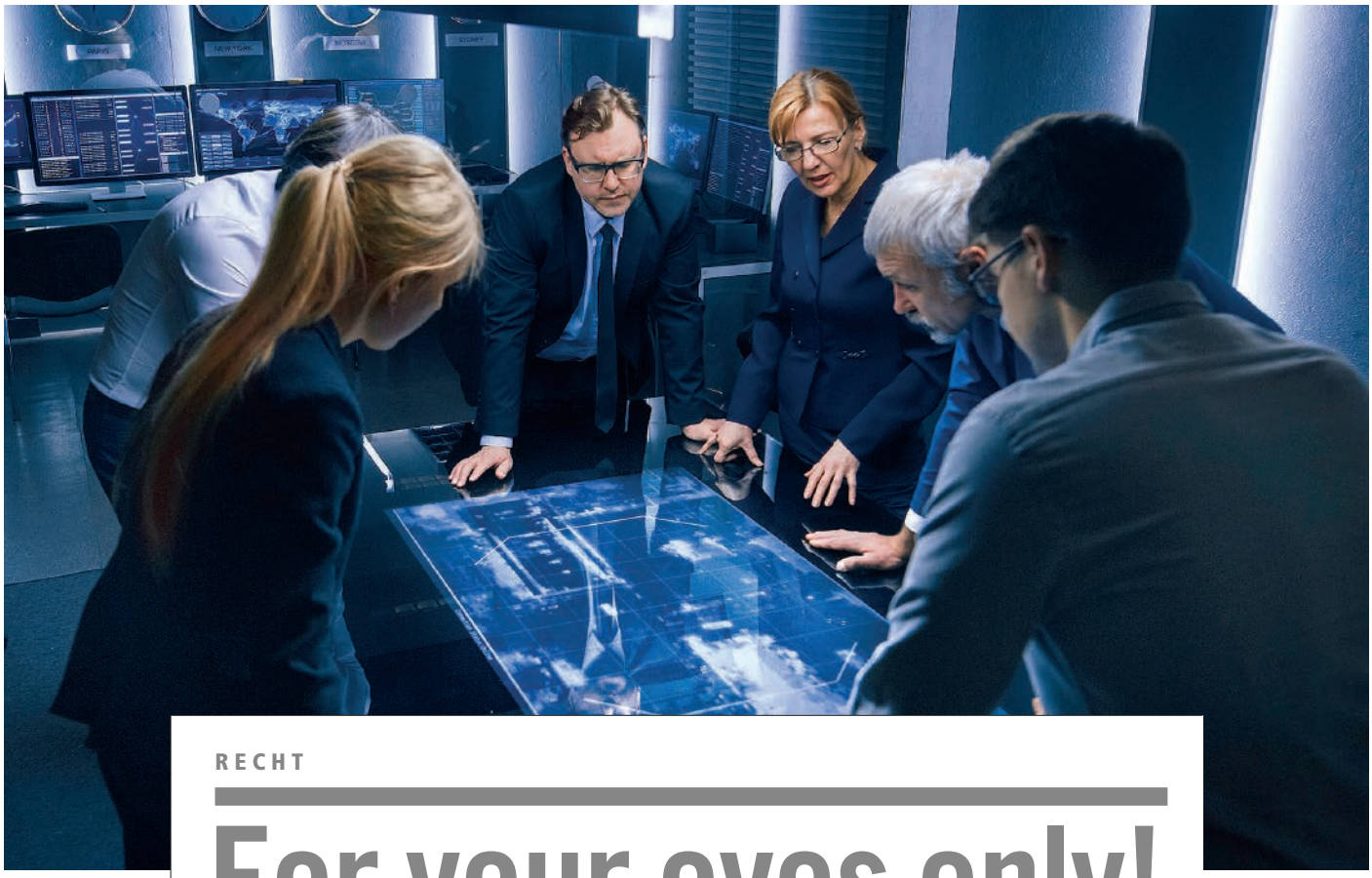

© Gorodenkoff - stock.adobe.com

RECHT

For your eyes only!

Schutz von Geschäftsgeheimnissen: Handlungspflichten nach dem neuen Geschäftsgeheimnisgesetz

Von der Unternehmensöffentlichkeit weitgehend unbeachtet ist bereits am 26. April 2019 das „Gesetz zum Schutz von Geschäftsgeheimnissen" (GeschGehG) in Kraft getreten. Basierend auf einer EU-Richtlinie enthält das Gesetz neue Begriffsbestimmungen, Verbote und Ausnahmen, erweiterte Ansprüche der Inhaber von Geschäftsgeheimnissen sowie Strafvorschriften, mit denen die bisherigen nebenstrafrechtlichen §§ 17 bis 19 UWG abgelöst werden. Ein Beitrag von Dr. Ulrich Dieckert, Rechtsanwalt in Berlin.

Nach der gesetzlichen Definition in § 2 Nr. 1 GeschGehG ist ein Geschäftsgeheimnis eine Information, die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Information umgehen, allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist. Unter diese Definition fallen klassische Betriebsgeheimnisse ebenso wie technisches Know-how oder betriebswirtschaftliche Daten. Beispiele für geschützte Informationen sind z. B. Geschäftszahlen, Kunden- und Lieferantendaten, Geschäftsstrategien, Preiskalkulationen, Herstellungsverfahren, Konstruktionspläne, Softwareprogramme etc. Die Informationen müssen gerade wegen ihrer fehlenden Offenkundigkeit von wirtschaftlichem Wert sein. Das ist anzunehmen, wenn die Erlangung, Nutzung oder Offenlegung ohne Zustimmung des Inhabers dessen wissenschaftliches oder technisches Potenzial, geschäftliche oder finanzielle Interessen, strategische Positionen oder Wettbewerbsfähigkeit negativ beeinflussen. Eines positiv festgestellten Marktwertes bedarf es nicht.

Angemessene Geheimhaltungsmaßnahmen

Zu einem gesetzlich geschützten Geschäftsgeheimnis werden diese Informationen jedoch nach der neuen gesetzlichen Definition erst, wenn sie auch „Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen" durch ihren rechtmäßigen Inhaber sind. Hier reichte bisher nach § 17 UWG ein erkennbarer „subjektiver Geheimhaltungswille" aus. Jetzt verlangt das Gesetz die Erfüllung einer nachweisbaren, objektiven Tatbestandsvoraussetzung, nämlich einer Geheimhaltungsmaßnahme. Die Nichtbeachtung dieser Vorgabe führt im Sinne eines „Umkehrschlusses" dazu, dass ein wirksamer gesetzlicher Schutz nicht besteht, wenn der rechtmäßige Inhaber keine auf die Geheimhaltung gerichteten vertraglichen, technischen und/oder organisatorischen Vorkehrungen getroffen hat. Nach der bisherigen Kommentierung des Gesetzes dürfen zwar keine überzogenen Anforderungen an die Angemessenheit der Schutzmaßnahmen gestellt werden. Es ist jedoch ein nachvollziehbares Geheimnis-Schutzkonzept umzusetzen. Ein solches Konzept sollte mindestens folgende Schritte enthalten:

- Erfassung aller im Unternehmen als geheimhaltungsbedürftig angesehenen Informationen
- Einteilung der Informationen in verschiedene Geheimhaltungskategorien nach Wichtigkeit und wirtschaftlicher Bedeutung
- Analyse des Informationsflusses im Unternehmen sowie Identifizierung möglicher Bedrohungen bzw. Angriffswege
- Entwicklung von Schutzmaßnahmen für jede Geheimhaltungskategorie
- Dokumentation aller Maßnahmen im Rahmen des Konzeptes (Beweislast liegt beim Geheimnisträger!)
- Schaffung von Aufmerksamkeit bei allen Mitarbeitern durch Schulungen und Compliance-Maßnahmen
- laufende Aktualisierung aller Maßnahmen (Follow-up)

Geeignete Schutzmaßnahmen

Geeignete Schutzmaßnahmen können organisatorischer Natur sein (klare Zuweisung von Verantwortlichkeiten für den Schutz von Information, Begrenzung des internen Zugriffs auf geheime Informationen nach dem „Need-to-know"-Prinzip, Trennung geheimnisträchtiger Abteilungen (z. B. F & E) von anderen Abteilungen) oder vertraglicher Art sein (z. B. Verschwiegenheitsvereinbarung mit Mitarbeitern, Abschluss von NDA-Vereinbarungen mit Geschäfts- und Vertragspartnern etc.). Insbesondere aber sind technische Maßnahmen zu ergreifen, um den Zugang und Zugriff auf Geschäftsgeheimnisse, die meist in elektronischer Form hinterlegt sind, zu verhindern. Solche Maßnahmen können zum Beispiel sein:

- Zugangskontrolle, Videoüberwachung, Alarmanlagen
- IT-Sicherheitsmaßnahmen: Verschlüsselung, Passwörter, Firewalls, Berechtigungskonzepte
- Kontrolle der Datenintegrität durch geeignete technische Systeme
- Trennung von Serverstrukturen etc.

Das größte Problem beim Schutz des eigenen Datenbestandes liegt häufig darin, dass man Angriffe von außen und schleichende Veränderungen der Daten bzw. deren Konfiguration gar nicht bemerkt. Gegenmaßnahmen werden daher i. d. R. erst dann ergriffen, wenn der Schaden schon angerichtet worden ist. Hiergegen helfen intelligente Softwarelösungen (Data-Integrity-Management), welche kleinste Veränderungen des Datenzustandes sofort anzeigen.

Ansonsten eröffnen die Vorgaben zum Geheimnisschutz neue Marktchancen für Anbieter aus der Sicherheitswirtschaft. Es empfiehlt sich jedenfalls, wenn Hersteller und Errichter sicherheitstechnischer Anlagen bzw. Unternehmen, die Sicherheitsdienstleistungen anbieten, ihre Kunden auf die erhöhten Anforderungen hinweisen und diese bei der Ertüchtigung ihrer Geheimnisschutzmaßnahmen unterstützen.

Haftung der Geschäftsführung

Wenn das Unternehmen keine angemessenen Maßnahmen ergreift, genießen die Geschäftsgeheimnisse keinen Schutz mehr, weil sie per gesetzlicher Definition keine solchen mehr sind. Das kann erhebliche wirtschaftliche Nachteile mit sich bringen, wofür auch die Geschäftsführungen der Unternehmen einstehen müssen. Denn diese haben nach den einschlägigen Vorschriften im GmbH- und Aktiengesetz die „Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden". Geschäftsführer, welche ihre Obliegenheiten verletzen, „haften der Gesellschaft solidarisch für den entstandenen Schaden" (vgl. § 43 Abs. 1, 2 GmbH-Gesetz, § 93 Abs. 1 und 2 Aktiengesetz). Vorliegend dürfte es gegen die Obliegenheiten bzw. Pflichten des Geschäftsleiters

Bitte umblättern ►

verstoßen, den nach § 2 Nr. 1b GeschGehG geforderten Geheimnisschutz zu vernachlässigen. Kommt es aufgrund mangelhafter/fehlender Maßnahmen zu einem Geheimnisverlust und damit wirtschaftlichem Schaden, kann das Unternehmen die Geschäftsführung auf Schadensersatz in Anspruch nehmen.

Verletzungshandlungen und Verbote

Die im Gesetz genannten Verletzungshandlungen und Verbote sind weit gefasst und dienen auch als Bezugspunkte für die späteren Strafvorschriften. Verboten ist sowohl die eigene Erlangung (§ 4 Abs. 1) als auch die Erlangung und spätere Nutzung und Offenlegung über andere Personen (z. B. durch Mitarbeiter oder sonstige Beauftragte, vgl. § 3 Abs. 3). Die unrechtmäßige Erlangung umfasst den unbefugten Zugang, die unbefugte Aneignung oder das unbefugte Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers unterliegen sowie jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht. Mit diesem Auffangtatbestand soll auch sonstiges geheimnisverletzendes Verhalten wie z. B. Vertragsbruch, Vertrauensbruch, Verleitung etc. erfasst sein. Verboten ist es nach § 4 Abs. 2 GeschGehG auch, wenn trotz entgegenstehender Verpflichtung (z. B. NDA-Vereinbarung) das anvertraute Geschäftsgeheimnis genutzt oder offengelegt wird.

Ausnahmen

Das neue Gesetz definiert jedoch nicht nur Verbote, sondern erlaubt auch explizite Ausnahmen. Dies betrifft zum einen das sogenannte „Reverse-Engineering" gemäß § 3 GeschGehG. Danach ist es jetzt ausdrücklich erlaubt, Produkte anderer Unternehmen zu beobachten, zu untersuchen, rückzubauen oder zu testen, um deren bis dahin nicht bekannte Konstruktion oder Funktionalität zu entschlüsseln. Dies gilt natürlich nur, wenn derartige Handlungen nicht individuell vertraglich verboten oder eingeschränkt sind, z. B. in Geheimhaltungsvereinbarungen oder F & E Vereinbarungen mit Geschäftspartnern. Ausgenommen ist zum anderen das sogenannte „Whistleblowing", welches durch §5 GeschGehG geschützt ist. Danach ist die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses zulässig, wenn dies zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens erfolgt, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen. Hiervon dürften Praktiken betroffen sein, die in den letzten Jahren in Deutschland für Aufsehen gesorgt haben, wie z. B. betrügerische Abgassoftware, illegale Steuersparmodelle, umweltschädliche Produktionsmethoden oder Umgehung gesetzlicher Sanktionsbestimmungen. Unternehmen ist anzuraten, für ein wirksames Meldesystem innerhalb des Betriebs zu sorgen (z. B. Bestellung von Ombudsleuten), damit die Mitarbeiter nicht jede Unregelmäßigkeit sogleich in die Öffentlichkeit tragen.

Ansprüche der Inhaber von Geheimnissen

Werden Geschäftsgeheimnisse unrechtmäßig verletzt, dann steht deren Inhabern nach dem neuen Gesetz ein ganzes Arsenal an Ansprüchen zur Verfügung. Das beginnt mit Beseitigungs- und Unterlassungsansprüchen gemäß § 6, die schon dann bestehen, wenn eine Rechtsverletzung erstmalig droht und endet noch lange nicht mit Ansprüchen auf Vernichtung, Herausgabe, Rückruf des rechtsverletzenden Produkts, dessen dauerhafte Entfernung aus den Vertriebswegen und/oder dessen Vernichtung (vgl. § 7). Der Verletzer kann gemäß § 11 des Gesetzes diese Ansprüche dem Inhaber in Geld abfinden, wenn er weder vorsätzlich noch fahrlässig gehandelt hat. Die Höhe der Abfindung in Geld bemisst sich nach der Vergütung, die im Falle einer vertraglichen Einräumung des Nutzungsrechtes angemessen gewesen wäre. Um die gesetzlichen Ansprüche überhaupt durchsetzen zu können, ist der Inhaber gemäß § 8 auch berechtigt, vom Rechtsverletzer zunächst Auskunft über die Herstellung und den Vertrieb der rechtsverletzenden Produkte sowie über Dokumente, Gegenstände, Materialien, Stoffe oder elektronische Dateien zu erlangen, die das Geschäftsgeheimnis enthalten oder verkörpern. Des Weiteren kann der Rechteinhaber nicht nur die Person, die das Geschäftsgeheimnis entwendet hat, in Anspruch nehmen, sondern auch das dahinter stehende Unternehmen, wenn der Beschäftigte/Beauftragte im unmittelbaren Zusammenhang mit den von ihm im Unternehmen wahrgenommenen Aufgaben gehandelt hat (vgl. § 12 GeschGehG). Schließlich stehen dem verletzten Inhaber von Geschäftsgeheimnissen auch Schadensersatzansprüche in Geld zu, wobei er zwischen drei Berechnungsmethoden wählen kann: der konkret entstandene Schaden, der Gewinn des Verletzers oder eine fiktive Nutzungsgebühr. Schadensersatzansprüche bestehen im Übrigen auch im Falle immaterieller Schäden (vgl. § 10 Abs. 3 GeschGehG).

Strafvorschriften

Schließlich enthält das neue Gesetz Strafandrohungen, die es in sich haben. So wird gemäß § 23 Abs. 1 mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geheimnis entgegen den Vorgaben aus § 4 erlangt, nutzt oder offenlegt; dies gilt ausdrücklich auch für Arbeitnehmer, denen solche Geschäftsgeheimnisse im Rahmen ihres Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden sind (vgl. § 23 Abs. 1 Nr. 3). Durch die Bezugnahme auf die Verbotsvorschriften aus § 4 wird klargestellt, dass nur strafbar sein kann, was zivilrechtlich nicht erlaubt ist. Bestraft wird im Übrigen nicht nur die eigene Beschaffung von Geschäftsgeheimnissen, sondern auch deren Nutzung und Offenlegung, wenn diese durch eine fremde Handlung erlangt wurde. Dadurch soll auch der Auftragsbeschaffung vorgebeugt werden. Schließlich wird das Vertrauen des Inhabers durch die Strafandrohung in § 23 Abs. 3 GeschGehG geschützt, wenn dieser das Geheimnis im geschäftlichen Verkehr geteilt hat (z. B. für eine gemeinsame Weiterentwicklung oder Verwertung) und von dem Empfänger gegen entsprechende Vertraulichkeitsvereinbarungen verstoßen wurde. Werden die o. a. Delikte gewerbsmäßig begangen oder handelt es sich um Industriespionage mit dem Ziel, das Geschäftsgeheimnis im Ausland zu nutzen, droht dem Täter eine Strafverschärfung bis zu fünf Jahren (§ 23 Abs. 4).

Fazit

Insgesamt sorgt das GeschGehG für eine deutliche Aufwertung des Geheimnisschutzes. Auf der anderen Seite zwingt es die Inhaber von Geheimnissen dazu, ihre „Kronjuwelen" angemessen vor fremdem Zugriff zu schützen. Die effektive Durchsetzung der im Gesetz geregelten Ansprüche hängt daher künftig auch davon ab, dass die Unternehmen entsprechende Geheimhaltungsmaßnahmen implementieren und nachweisen können. Dabei sollten die Geschäftsführungen im eigenen Haftungsinteresse dafür sorgen, dass dies auch geschieht. Für die Anbieter von Sicherheitstechnik und Sicherheitsdienstleistungen eröffnet das Gesetz neue Marktchancen, die genutzt werden sollten. ■

Kontakt

Dr. Ulrich Dieckert Rechtsanwalt
Berlin
Tel.: +49 30 278 707
ulrich.dieckert@dieckert.de
www.dieckert.de