Deloitte.

URL: http://www.deloitte-tax-news.de/unternehmensrecht/das-neue-geschaeftsgeheimnisschutzgesetz-und-seine-auswirkungen-fuer-die-praxis.html

29.08.2019

Unternehmensrecht

Das neue Geschäftsgeheimnisschutzgesetz und seine Auswirkungen für die Praxis

Mit dem neuen Geschäftsgeheimnisschutzgesetz („GeschGehG") hat der deutsche Gesetzgeber den Schutz von Geschäftsgeheimnissen einer vollständigen Neuregelung zugeführt. Das Gesetz zieht ggf. erheblichen Handlungsbedarf nach sich – nicht nur für Technologieunternehmen.

Einführung
Am 26.04.2019 ist das neue Geschäftsgeheimnisschutzgesetz („GeschGehG") in Kraft getreten. Deutschland hat damit, wenn auch mit einiger Verspätung, die Vorgaben der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung in nationales Recht umgesetzt.

Bislang war der Schutz von Geschäftsgeheimnissen lediglich fragmentarisch geregelt.

Das neue GeschGehG definiert erstmals den Begriff des Geschäftsgeheimnisses, kodifiziert ein ausdifferenziertes System von Ansprüchen des Geheimnisinhabers und nimmt auch ausdrücklich Bezug auf Grenzen des gesetzlichen Schutzes – etwa für Whistleblower oder bei journalistischer Tätigkeit.

Unternehmen ist dringend anzuraten, unverzüglich Maßnahmen einzuleiten, um den Schutz ihrer Geschäftsgeheimnisse zu systematisieren, konkretisieren, kontrollieren und dokumentieren. Der nachfolgende Beitrag gibt einen Überblick über die gesetzlichen Neuerungen und zeigt den mit ihnen einhergehenden Handlungsbedarf für Unternehmen auf.

Die Ausgangslage
Geschäftsgeheimnisse sind nicht nur für technologieintensive Unternehmen von immenser wirtschaftlicher Bedeutung. Vielmehr ist es für Unternehmen aller Branchen essentiell, vorhandenes Know-how, Produktspezifikationen, Kundendaten, Ergebnisse von Markt- und Verhaltensanalysen, Preise und eine Vielzahl anderer Informationen zu schützen.

Bislang war der Schutz von Geschäftsgeheimnissen im deutschen Recht Gegenstand unterschiedlicher, über diverse Gesetze verstreuter Vorschriften und wurde gar als das Aschenputtel des geistigen Eigentums bezeichnet.

Bei den bislang anwendbaren Strafvorschriften sind hier unter anderem die §§ 17 bis 19 UWG sowie die §§ 201 bis 206 StGB, welche die Verletzung des persönlichen Lebens- und Geheimbereichs unter Strafe stellen, zu nennen. Das Zivilrecht kannte demgegenüber keine ausdrücklichen den Schutz von Geschäftsgeheimnissen betreffenden Regelungen. Bei rechtswidriger Verletzung von Geschäftsgeheimnissen kamen etwa vertragliche Schadensersatzansprüche nach §§ 280 Abs. 1, 241 Abs. 2 BGB sowie deliktische Ansprüche gemäß §§ 823 Abs.1, 826 bzw. § 823 Abs.2 BGB in Verbindung mit einem jeweils verwirklichten drittschützenden Schutzgesetz in Betracht. Zur Begründung von Unterlassungsansprüchen wurden die Bestimmungen der §§ 823, 1004 BGB analog herangezogen. Besondere Verfahrensvorschriften für Geschäftsgeheimnisse betreffende Streitigkeiten existierten nicht.

Mit der Umsetzung der Richtlinie (EU) 2016/943 durch das GeschGehG wurde nunmehr erstmals ein neues Stammgesetz geschaffen, dass den Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung zum Gegenstand hat (§ 1 Abs. 1 GeschGehG).

Der neue „Geschäftsgeheimnis"-Begriff
Das GeschGehG legt erstmals fest, was unter einem Geschäftsgeheimnis zu verstehen ist. Gemäß § 2 Nr. 1 GeschGehG ist Geschäftsgeheimnis eine Information, (i) 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 (mithin geheim) und daher von

wirtschaftlichem Wert ist und (ii) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und (iii) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Geheime Informationen

Das GeschGehG differenziert nicht nach der Art der Information. Dem Schutz des GeschGehG unterfallen können damit höchst unterschiedliche Informationen wie zum Beispiel Businesspläne, Werbestrategien und Kundenlisten aber natürlich auch Konstruktionspläne, Rezepturen, Prototypen, Verfahren, etc. Ein ausdrücklicher Unternehmensbezug ist nicht verlangt.

Ob die Information geheim ist, bestimmt sich nach einem relativen Geheimnisbegriff, nämlich nach der Kenntnis bzw. Kenntnisnahmemöglichkeit von Personen, die üblicherweise mit Information der fraglichen Art umgehen.

Wirtschaftlicher Wert

Auch im Hinblick auf die in der EU-Richtlinie niedergelegten Erwägungsgründe ist das Kriterium des wirtschaftlichen Werts weit zu verstehen. Es kann dem Grundsatz nach auch bei sogenannten negativen Informationen erfüllt sein, etwa wenn es um geheime Informationen geht, die ihren rechtmäßigen Inhaber belasten. Ob und inwieweit ein Geheimnisschutz bei Informationen über Rechtsverletzungen bestehen kann, ist umstritten.

Angemessene Geheimhaltungsmaßnahmen

Eine wesentliche durch das Gesetz begründete Neuerung besteht darin, dass derjenige, der Ansprüche aus der Verletzung eines Geschäftsgeheimnisses geltend machen möchte, nunmehr nachweisen muss, dass er sich bemüht hat, den Umständen nach angemessene (betriebsinterne) Geheimhaltungsmaßnahmen einzuführen. Hierin ist eine Verschärfung der bisherigen Anforderungen an den Geheimnisschutz zu sehen, da die gesetzliche Regelung im Umkehrschluss darauf hinausläuft, dass ein wirksamer gesetzlicher Schutz gegen Geheimnisverrat nicht besteht, wenn der rechtmäßige Inhaber keine auf eine Geheimhaltung gerichteten vertraglichen, technischen und/oder organisatorischen Vorkehrungen getroffen hat.

Da das als Obliegenheit zu verstehende Kriterium der Angemessenheit der zu treffenden Geheimhaltungsmaßnahmen weder im Gesetzestext noch in der bisherigen Rechtsprechung eine Konkretisierung erfahren hat, ist eine abschließende Aussage zur Bedeutung dieses Kriteriums gegenwärtig noch nicht möglich. Anhaltspunkte für die Auslegung können Erfahrungen mit vergleichbaren Bestimmungen in anderen Rechtsordnungen bieten. Auch diese führen allerdings nicht zu einer abschließenden Antwort auf die Frage, was getan werden muss, damit die vorgenommenen Geheimhaltungsmaßnahmen als angemessen angesehen werden. Vielmehr muss im jeweiligen Einzelfall eine Antwort auf diese Frage gefunden werden.

Die Angemessenheit der zu treffenden Maßnahmen dürfte hierbei insbesondere von Faktoren wie der Art der Information sowie ihrer Bedeutung und ihrem Wert für das Unternehmen, aber auch von der Größe des Unternehmens, und der Kosten und Üblichkeit der jeweiligen Maßnahmen abhängen. Um eine Handhabbarkeit zu erreichen, empfiehlt es sich, das vorhandene geheimhaltungsbedürftige Know-how zu bewerten und entsprechend zu kategorisieren. Ziel sollte es dabei sein, ein für das jeweilige Unternehmen passendes Geheimnisschutzkonzept zu entwickeln.

Bausteine eines derartigen Konzeptes könnten etwa die Folgenden sein:

- Erfassung aller im Unternehmen als geheimhaltungsbedürftig angesehenen Informationen.
- Einteilung dieser Informationen in verschiedene Geheimhaltungskategorien nach ihrer Wichtigkeit und wirtschaftlichen Bedeutung für das Unternehmen.
- Entwicklung von Schutzmaßnahmen für jede Geheimhaltungskategorie. Beispielhaft seien hier die Durchsetzung des „Need-to-know"-Prinzips, die eindeutige Kennzeichnung von geheimhaltungsbedürftigen Informationen, Schaffung von zugangsgesicherten Räumlichkeiten, Installation von Alarmanlagen und Videoüberwachung, Verwendung von speziellen Verschlüsselungen und Passwörtern, die Einrichtung von Gruppenberechtigungen sowie weitere IT-Sicherheitsmaßnahmen wie etwa Firewalls oder ein Verbot der Nutzung privater Speichermedien, aber auch der Abschluss von geeigneten Vertraulichkeitsvereinbarungen mit Arbeitnehmern, Kunden bzw. Lieferanten sowie Kooperationspartnern genannt.

Sofern möglich, sollten die einzelnen Maßnahmen im Rahmen des

Geheimnisschutzkonzeptes schriftlich niedergelegt werden, damit eine auch im Streitfall beweisfähige Dokumentation vorliegt. Darüber hinaus dürfte es sich empfehlen, zumindest eine für den Geheimnisschutz im Unternehmen verantwortliche Person zu benennen.

Um auch innerhalb der Belegschaft eine Sensibilität für die Sinnhaftigkeit und den Wert von Geheimnisschutzmaßnahmen zu erzeugen, sollten Schulungen zum Umgang mit Geschäftsgeheimnissen erfolgen. Dabei sollte der Fokus nicht einseitig auf das Ergreifen rechtzeitiger Schutzmaßnahmen, etwa hinsichtlich des bei der Entwicklung neuer Produkte und Dienstleistungen entstehenden Know-hows, gelegt werden; ebenso wichtig ist es - vor dem Hintergrund des durch das GeschGehG modifizierten Haftungskonzepts - Mitarbeiter darauf hinzuweisen, dass bei der Einstellung von Mitarbeitern oder der Begründung von Kooperationen Know-how nicht in rechtswidriger Weise in die Unternehmenssphäre gelangen darf.

Berechtigtes Interesse an der Geheimhaltung

Mit dem nach dem Gesetzeswortlaut erforderlichen „berechtigten Interesse an der Geheimhaltung" hat der deutsche Gesetzgeber eine in der zugrundeliegenden EU-Richtlinie nicht vorgesehene zusätzliche Voraussetzung statuiert. Die Einführung dieser zusätzlichen Voraussetzung war (wohl), von dem Wunsch getragen, Informationen über Rechtsverletzungen vom Geheimnisschutz ausnehmen zu können und zugleich in der Befürchtung begründet, mit der Neuregelung eine Beschränkung investigativer journalistischer Tätigkeit herbeizuführen. Da die zugrundeliegende EU-Richtlinie hier anderen Prinzipien folgt und öffentliche Interessen im Rahmen der – im GeschGehG in § 5 geregelten – Ausnahmen, nicht dagegen bei der Geheimnisdefinition, berücksichtigt, stößt das Vorgehen des deutschen Gesetzgebers in der Literatur auf Kritik und wird diskutiert, ob die entsprechende Voraussetzung richtlinienwidrig, jedenfalls aber richtlinienkonform auszulegen ist.

Weitreichende Ansprüche für Inhaber von Geschäftsgeheimnissen
Das GeschGehG gibt dem geschädigten Inhaber von Geschäftsgeheimnissen ein umfangreiches Repertoire an Handlungsmöglichkeiten an die Hand.

So sieht das Gesetz Ansprüche auf Beseitigung und Unterlassung (§ 6 GeschGehG) sowie auf Herausgabe, Rückruf und Entfernung aus den Vertriebswegen sowie die Vernichtung und Rücknahme der rechtsverletzenden Produkte (§ 7 GeschGehG) vor. Flankiert werden diese Ansprüche jeweils von einem Auskunftsanspruch gegen den Rechtsverletzer (§ 8 GeschGehG).

Zu beachten ist in diesem Zusammenhang, dass die genannten Ansprüche auch gegenüber dem neuen Arbeitgeber eines ehemaligen Mitarbeiters geltend gemacht werden können, sofern der betreffende Mitarbeiter Geschäftsgeheimnisse durch Mitnahme oder Offenlegung verletzt hat und damit Rechtsverletzer ist (§ 12 GeschGehG). Einschränkungen bestehen für die Haftung auf Schadenersatz für eine unzureichende Auskunftserteilung.

Der durch das GeschGehG erweiterte Katalog von Ansprüchen bringt im Vergleich zur bisherigen Rechtslage eine deutliche Besserstellung des Inhabers eines verletzten Geschäftsgeheimnisses mit sich. Erwähnenswert ist in diesem Zusammenhang der Umstand, dass der in einer gerichtlichen Auseinandersetzung obsiegenden Partei nunmehr grundsätzlich auf Antrag in der Urteilsformel die Befugnis zugesprochen werden kann, das Urteil oder Informationen über das Urteil auf Kosten der unterliegenden Partei öffentlich bekannt zu machen, wenn die obsiegende Partei hierfür ein berechtigtes Interesse darlegt (§ 21 GeschGehG).

Die Möglichkeit zur Bekanntmachung des Urteils in Geschäftsgeheimnisstreitsachen, gleich welchen Rechtswegs, dient der Abschreckung potentieller Rechtsverletzer und der Unterrichtung der Öffentlichkeit über die rechtswidrige Nutzung oder Offenlegung von Geschäftsgeheimnissen. Entsprechende Regelungen bestehen bereits in § 12 Absatz 3 UWG, § 103 UrhG, § 19c MarkenG, § 140e PatG und § 24e Gebrauchsmustergesetz.

Was die strafrechtliche Relevanz der Verletzung von Geschäftsgeheimnissen angeht, wurden die bislang geltenden Straftatbestände der §§ 17 bis 19 UWG ohne wesentliche Änderungen in § 23 GeschGehG überführt.

Schrankenregelungen
Auch der durch das neue Gesetz erweiterte Schutz von Geschäftsgeheimnissen ist jedoch keinesfalls absolut. So kodifiziert § 5 GeschGehG Ausnahmetatbestände, unter denen die Erlangung, Nutzung und Offenlegung eines Geschäftsgeheimnisses gerechtfertigt sein kann und der Geheimnisschutz hinter Belange des Allgemeinwohls zurücktreten muss. Das dafür erforderliche berechtigte Interesse kann grundsätzlich jedes von der Rechtsordnung

gebilligte Interesse sein. Nach § 5 GeschGehG fällt die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses nicht unter das Handlungsverbot nach § 4 GeschGehG, wenn dies

- dem Schutz der Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit, einschließlich der Achtung der Freiheit und der Pluralität der Medien, dient (§ 5 Nr.1 GeschGehG);
- zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens dient, sofern die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen (§ 5 Nr. 2 GeschGehG, Whistleblower-Fälle) - bei der Organisation unternehmensinterner Hinweisgebersysteme sind neben der Bestimmung des § 5 Nr. 2 GeschGehG die Vorgaben der zeitnah in Kraft tretenden Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (EU 2018/0106), zu berücksichtigen;
- im Rahmen der Offenlegung durch Arbeitnehmer gegenüber der Arbeitnehmervertretung dient, wenn dies erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann (§ 5 Nr. 3 GeschGehG). Hierzu könnte etwa die Verfolgung legitimer Gruppeninteressen zählen, zum Beispiel, wenn die Arbeitnehmervertretung über einen bevorstehenden Personalabbau unterrichtet.

Reverse Engineering
Bislang bestand im deutschen Recht ein grundsätzlicher Schutz vor einem „Reverse Engineering“ durch Dritte. Darunter ist der Rückbau und die Analyse eines Objektes mit dem Ziel zu verstehen, den Aufbau des Objektes und das in diesem enthaltene, nicht offen einsehbare, Know-how in Erfahrung zu bringen. Ratio dieses Verbots war, dass es aus wettbewerbsrechtlicher Sicht als durchaus erstrebenswert angesehen wurde, dass sich Dritte Know-how nicht einfach aneignen dürfen sollen, insbesondere da dies aufgrund entsprechend ausgereifter Analysemöglichkeiten und -geräte tendenziell immer einfacher und schneller möglich ist.

Nachdem dieses Verbot in der Vergangenheit bereits aufgeweicht worden war, indem es nicht mehr auf Fälle angewandt wurde, in denen ein „Reverse Engineering“ ohne größere Schwierigkeiten durchführbar war, gelten solche Handlungen nach der gesetzlichen Neuregelung nunmehr vielfach als erlaubt, sofern die Tatbestandsvoraussetzungen des § 3 Abs. 1 Nr. 2 GeschGehG erfüllt sind. Dies ist der Fall, wo ein Geschäftsgeheimnis erlangt wurde durch „ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der (i) öffentlich verfügbar gemacht wurde oder (ii) sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt“.

Vor diesem Hintergrund können Unternehmen – je nach Einzelfall – weiterhin Schutz vor den Folgen des „Reverse Engineerings“ etwa unter Berufung auf die Bestimmungen des Urheber-, Patent- und Lauterkeitsrecht suchen oder aber versuchen, Reverse Engineering-Tatbestände durch spezielle vertragliche Regelungen zu unterbinden. Allerdings ist fraglich, ob derartige vertragliche Beschränkungen rechtswirksam und mit Wirkung gegen die richtigen Parteien vereinbart werden können.

Prozessuale Besonderheiten
Im Rahmen von Geschäftsgeheimnisstreitsachen haben die staatlichen Gerichte nunmehr die Möglichkeit, Maßnahmen zum Schutz der streitgegenständlichen Geschäftsgeheimnisse zu treffen (§§ 16ff. GeschGehG). Zu den möglichen Maßnahmen zählen etwa die Auferlegung von Verschwiegenheitsverpflichtungen gegenüber Parteien, ihren Prozessvertretern, Zeugen, Sachverständigen und sonstige Vertreter bzw. Personen. Bei Zuwiderhandlungen gegen die hierdurch begründeten Verpflichtungen kann zudem ein Ordnungsgeld bis zu EUR 100.000,00 oder Ordnungshaft bis zu sechs Monaten festgesetzt und sofort vollstreckt werden. Zudem kann etwa auch die Parteiöffentlichkeit auf einen begrenzten Personenkreis eingeschränkt werden, um das streitgegenständliche Geschäftsgeheimnis zu schützen.

Schutz von Algorithmen (in Big Data-Anwendungen)
Zu den durch das neue GeschGehG eröffneten Möglichkeiten zum Schutz von Algorithmen sei auf das Interview mit Frau Rechtsanwältin Dr. Katharina Scheja, Deloitte Legal Frankfurt sowie deren Beitrag in CR | Computer und Recht, 8/2018, S. 485 – 552 verwiesen.

Fazit
Wenngleich das neue GeschGehG keinen gesetzlichen Umsetzungszwang vorsieht, sollten Unternehmen ein tragfähiges Konzept zum Schutz ihrer Geschäftsgeheimnisse entwickeln,

um sich im Streitfall effektiv gegen Rechtsverletzungen verteidigen zu können. Ein solches Konzept sollte dabei unbedingt schriftlich dokumentiert werden. Die möglichen Maßnahmen zum Schutz von Geschäftsgeheimnissen sind dabei vielfältig und sind nach Maßgabe des jeweils einschlägigen Einzelfalls festzulegen. Neben vertraglichen Vereinbarungen und organisatorischen Regelungen kommen hierfür insbesondere auch technische Sicherungsvorkehrungen in Betracht. Besondere Vorkehrungen sind auch vor dem Hintergrund der weiteren Liberalisierung des Reverse Engineering angezeigt.

---

www.deloitte-tax-news.de

Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie hat nicht den Sinn, Grundlage für wirtschaftliche oder sonstige Entscheidungen jedweder Art zu sein. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. Sollte jemand Entscheidungen jedweder Art auf Inhalte dieser Mandanteninformation oder Teile davon stützen, handelt dieser ausschließlich auf eigenes Risiko. Deloitte GmbH übernimmt keinerlei Garantie oder Gewährleistung noch haftet sie in irgendeiner anderen Weise für den Inhalt dieser Mandanteninformation. Aus diesem Grunde empfehlen wir stets, eine persönliche Beratung einzuholen.

This client information exclusively contains general information not suitable for addressing the particular circumstances of any individual case. Its purpose is not to be used as a basis for commercial decisions or decisions of any other kind. This client information does neither constitute any advice nor any legally binding information or offer and shall not be deemed suitable for substituting personal advice under any circumstances. Should you base decisions of any kind on the contents of this client information or extracts therefrom, you act solely at your own risk. Deloitte GmbH will not assume any guarantee nor warranty and will not be liable in any other form for the content of this client information. Therefore, we always recommend to obtain personal advice.