Sonderausgabe zum neuen Geschäftsgeheimnisgesetz

VBB RECHTSANWÄLTE

news.wirtschaftsstrafrecht.de

01 | **2019** **Wirtschaftsstrafrecht in der Beraterpraxis**

Das neue Geschäftsgeheimnisgesetz

Pflichten und Risiken für Unternehmensjuristen

Am 26.04.2019 ist – mit knapp einjähriger Verspätung – das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG, BGBl. I S. 466) in Kraft getreten. Dieses Gesetz enthält in § 2 Nr. 1 GeschGehG erstmals eine gesetzliche Definition des Begriffs „Geschäftsgeheimnis". Ein Geschäftsgeheimnis ist eine außerhalb des Unternehmens nicht offenkundige Information, an deren Geheimhaltung das Unternehmen ein berechtigtes Interesse hat und die *„Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist".*

1. Geheimhaltungsmaßnahmen als konstitutive Voraussetzung eines Geschäftsgeheimnisses

Insbesondere die Merkmale der Nichtoffenkundigkeit und des Geheimhaltungsinteresses waren bereits Bestandteil der bisherigen Definition des Geschäftsgeheimnisses. Allerdings wird künftig auf das bislang verwendete subjektive Merkmal des Geheimhaltungswillens zu Gunsten des objektiven Merkmals der angemessenen Geheimhaltungsmaßnahmen verzichtet, was zu einer deutlichen Verschärfung der Anforderungen an ein Geschäftsgeheimnis führt. Nunmehr obliegt es dem Unternehmen, die Informationen zu ermitteln, die ein Geschäftsgeheimnis darstellen sollen und diese durch entsprechende Maßnahmen zu schützen. Fehlt es an Schutzmaßnahmen, handelt es sich bei der Information – selbst wenn sie das Kernstück der Produktion oder des Vertriebs eines Unternehmens darstellt – nicht um ein Geschäftsgeheimnis. Ein zivil- oder strafrechtlicher Schutz einer solchen Information durch das GeschGehG besteht nicht – die Information kann durch (ehemalige) Mitarbeiter des Unternehmens oder Konkurrenten (weitgehend) frei verwendet werden. Hierbei sind die betroffenen Unternehmen als Geheimnisinhaber für das Vorliegen angemessener Sicherungssysteme beweisbelastet.

2.„Erforderliche" und„angemessene" Sicherungsmaßnahmen"

Fest steht somit, dass Unternehmen ihre Geschäftsgeheimnisse nunmehr durch „angemessene" und „erforderliche" Sicherungssysteme vor unbefugten Zugriff schützen müssen. Unklar bleibt insoweit, welche Maßnahmen hierfür erforderlich und angemessen sind und für welches Schutzniveau der Geheimnisinhaber demnach beweisbelastet ist. Die Gesetzesbegründung stellt hierzu klar, dass nicht *„jede geheim zu haltende Tatsache gesondert zu kennzeichnen [ist], sondern es können grundsätzliche 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".*

In die Bewertung der Angemessenheit einer Geheimhaltungsmaßnahme sollen insb. der Wert des Geheimnisses, die Entwicklungskosten, die Natur der Information, die Bedeutung für das Unternehmen, die Größe des Unternehmens, die üblichen Geheimhaltungsmaßnahmen im Unternehmen, die Art der Kennzeichnung der Information und die vereinbarten vertraglichen Regelungen mit Arbeitnehmern und Geschäftspartnern einfließen. Bereits diese durch den Gesetzgeber aufgeführten Kriterien zeigen, dass es auch künftig kein einheitliches – für alle Unternehmen gültiges – Konzept

weiter auf Seite 2

In dieser Sonderausgabe:

von angemessenen Geheimhaltungsmaßnahmen geben wird. Denn das, was als angemessen bewertet wird, wird je nach Unternehmensgröße, Tätigkeitsgebiet, Spezialisierungsgrad etc. variieren.

3. Unmittelbare Handlungserfordernisse für die Praxis

Spätestens mit dem Inkrafttreten des GeschGehG gilt es für Unternehmen, sich auf die neuen Vorgaben zum Geheimnisschutz einzustellen und Geheimhaltungsmaßnahmen zu implementieren oder bestehende Sicherungssysteme auf Ihre Wirksamkeit hin zu überprüfen - und zwar bevor kritisches Wissen in signifikantem Umfang aus dem Unternehmen abfließt. Hierzu sollten Unternehmen in einem ersten Schritt bestehende Risiken identifizieren und eruieren, welche Informationen in welchem Umfang gefährdet sind und von welchen Personen eine solche Gefährdung ausgehen könnte.

In einem zweiten Schritt sollten die so identifizierten geheimen Informationen klassifiziert werden, um jeweils „angemessene" Geheimhaltungsmaßnahmen zu implementieren. Hierbei bietet sich ein mehrstufiges System an, das von den „Kronjuwelen" des Unternehmens bis zu sensiblen Informationen reicht. Welche Informationen hierbei in welche Kategorie fallen, hängt wiederum von Größe, Marktposition und der Tätigkeitssparte des Unternehmens ab.

Neben der Identifizierung der relevanten Geheimnisse eines Unternehmens müssen auch mögliche Angriffswege durch externe „Betriebsspione" und erfahrungsgemäß von besonderer Bedeutung, durch eigene Mitarbeiter identifiziert werden, um sinnvolle Schutzmaßnahmen zu erarbeiten. Zuletzt muss der Geheimnisschutz so organisiert werden, dass einerseits die Arbeitsfähigkeit des Unternehmens sichergestellt und andererseits effektive Zugriffsbeschränkungen implementiert werden. Dies setzt neben technischen insbesondere auch arbeitsrechtliche Maßnahmen sowie Vorgaben zum Umgang mit Geschäftsgeheimnissen bei der täglichen Arbeit voraus.

Weitere Aufgaben für Unternehmen

Die EU Whistleblower-Richtlinie

Kaum hat der deutsche Gesetzgeber das GeschGehG verabschiedet, legt die EU in Bezug auf Geheimnisschutz und Whistleblowing eine weitere ***„Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden"*** (sog. Whistleblower-Richtlinie) vor. Ziel der Richtlinie ist es primär, Personen zu schützen, die im Rahmen ihrer Arbeitsbeziehungen auf Verletzungen und Gefährdungen öffentlicher Interessen hinweisen oder Informationen hierzu öffentlich machen.

Daneben wird als eines der Kernstücke der Richtlinie aber auch die Verpflichtung für Unternehmen implementiert, sichere, vertrauliche und effektive Meldesysteme bereitzustellen. So soll potentiellen Whistleblowern im Unternehmen die Möglichkeit eingeräumt werden, sich mit der Meldung von etwaigen Verstößen zunächst an einen unternehmensinternen oder durch das Unternehmen beauftragten Dritten zu wenden, bevor sie mit den zuständigen Behörden in Kontakt treten. Eine solche interne Meldung von Verstößen und die damit einhergehende Möglichkeit, diese etwaig ohne die Einschaltung von Behörden prüfen und ggf. abstellen zu können, hat bereits viele Unternehmen animiert, entsprechende Hinweisgebersystem einzurichten.

Mit der – in zwei Jahren zu erwartenden – Umsetzung der Richtlinie in nationales Recht wird es aber erstmals eine Verpflichtung zur Einrichtung eines solchen Systems und dezidierte Vorgaben zu dessen Ausgestaltung geben.

1. Verpflichtung zur Bereitstellung von Hinweisgebersystemen

Durch die Richtlinie werden juristische Personen des Privat- und des öffentlichen Rechts verpflichtet, interne Meldekanäle einzurichten werden, die Meldungen eigener Mitarbeiter wie auch externer Personen – wie z. B. Mitarbeitern von Subunternehmern und Zulieferern – ermöglichen.

Eine Rechtspflicht zur Einrichtung von Hinweisgebersystemen soll im privatwirtschaftlichen Sektor alle Unternehmen mit mehr als 50 Mitarbeitern treffen. Es wird allerdings in das Ermessen der Mitgliedsstaaten gestellt, nach einer angemessenen Risikobewertung unter Berücksichtigung des Unternehmensgegenstandes und des hieraus resultierenden Risikoniveaus, auch kleinere juristische Personen einzuschließen. Juristischen Personen des Privatrechts mit 50 bis 249 Beschäftigten soll die Möglichkeit eingeräumt werden, sich ein Whistleblower-System zu „teilen", soweit die Vertraulichkeit der Meldung, deren Bearbeitung und die Behebung von etwaigen Verstößen hierdurch nicht beeinflusst wird.

Für juristische Personen des öffentlichen Rechts, einschließlich Gemeinden und kommunalen Unternehmen, soll grundsätzlich eine Verpflichtung zur Einrichtung eines Meldesystems bestehen, wobei den Mitgliedsstaaten die Möglichkeit zur Befreiung von kleineren Gemeinden

mit weniger als 10.000 Einwohnern und Unternehmen mit weniger als 50 Mitarbeitern eingeräumt wird. Auch hier soll die Möglichkeit eines kooperativ betriebenen Meldesystems mehrerer juristischer Personen bzw. des Rückgriffs auf eine zentrale Meldestelle bestehen.

2. Ausgestaltung von Hinweisgebersystemen

Die konkrete Ausgestaltung des internen Meldesystems wird europarechtlich ebenfalls vorgegeben. So müssen die einzurichtenden Meldekanäle eine schriftliche, mündliche – über eine Telefonhotline oder andere Sprachnachrichtensysteme – sowie auf Anfrage des Meldenden auch eine Meldung im persönlichen Gespräch in angemessener Frist ermöglichen. Über die Bereitstellung dieser Meldekanäle, einschließlich der Möglichkeit, etwaiges unternehmensrelevantes Fehlverhalten auch extern an die zuständigen Behörden zu adressieren, sind die Mitarbeiter über leicht zugängliche und klare Informationssysteme zu unterrichten.

Darüber hinaus muss das Unternehmen interne Zuständigkeitsregelungen für die Entgegennahme und Bearbeitung von eingehenden Meldungen treffen. Konkret ist eine geeignete und unparteiische Person oder Abteilung im Unternehmen zu benennen, in deren Zuständigkeit die Bearbeitung und sorgfältige Prüfung der Meldung fällt, die in Kontakt mit dem Meldenden steht und diesen – innerhalb von drei Monaten – über den Fortgang der Untersuchung unterrichtet. Der Verantwortliche muss in der Lage sein, unmittelbar an die Geschäftsführung des Unternehmens zu berichten. Die Pflicht zur Benennung eines eigenständigen „Whistleblowing-Beauftragten" ist hiermit aber (noch) nicht verbunden, vielmehr soll es z.B. dem CCO, dem Rechts- oder Datenschutzbeauftragten oder einem Geschäftsleitungsmitglied möglich sein, diese Aufgabe zu übernehmen. Vor dem Hintergrund dieser umfangreichen Verpflichtungen des Unternehmens ist jedoch zu berücksichtigen, dass diese die Implementierung eines funktionsfähigen Hinweisgebersystems nicht zwingend selbst vornehmen müssen. Vielmehr sieht die Richtlinie ausdrücklich vor, dass der Betrieb des Systems – als für Unternehmen durchaus attraktive Alternative an externe Dienstleister – beispielsweise Rechtsanwaltskanzleien – ausgelagert werden kann, soweit diese Gewähr für die Einhaltung der Vorgaben zu Unabhängigkeit, Datenschutz und Vertraulichkeit bieten.

Bei Einrichtung eines Hinweisgebersystems ist weiterhin sicherzustellen, dass die Identität des Meldenden geschützt und die Vertraulichkeit der Meldung gewahrt wird. Dies gilt auch dann, wenn im Falle von anonymen Meldungen die Identität im Laufe des Verfahrens aufgedeckt wird. Ergänzend sind auch die Vorgaben der DSGVO im Rahmen der Bearbeitung von Whistleblower-Meldungen einzuhalten.

... und nicht zuletzt:

Der Datenschutz

Der Aspekt des Datenschutzes darf im Rahmen der Diskussion über Geheimnis- und Whistleblowerschutz selbstverständlich nicht übersehen werden.

1. Urteil des LAG Baden-Württemberg

Dies verdeutlicht auch ein Urteil des LAG Baden-Württemberg 20.12.2018 (Az.: 17 Sa 11/18). Hintergrund des Urteils war ein arbeitsgerichtlicher Streit zwischen einem Automobilunternehmen und einem bei dem Konzern angestellten Unternehmensjuristen, in dessen Verlauf sich herausgestellt hat, dass es zu dem (gekündigten) Mitarbeiter auch einen Vorgang im unternehmensinternen Hinweisgebersystem gab, der auf die Meldung eines Whistleblowers zurückgegangen sein könnte. Der gekündigte Mitarbeiter hatte beantragt, eine vollständige Kopie dieses Vorgangs zu erhalten und Ansprüche hierzu u.a. aus der DSGVO abgeleitet.

Das LAG hat diesem Anspruch stattgegeben und festgestellt, dass ein Arbeitnehmer gemäß Art. 15 Absatz 1 DSGVO Auskunft und gemäß Artikel 15 Abs. 3 S. 1 DSGVO eine Kopie der durch den Arbeitgeber über ihn gespeicherten personenbezogenen Daten verlangen kann. Der Arbeitgeber könne die Erfüllung des Anspruchs nur in dem Umfang verweigern, wie durch die Auskunft Informationen offenbart würden, die geheimhal-

weiter auf Seite 4

Weitere News

- In eigener Sache: VBB Rechtsanwälte eröffnet dritten Standort in Karlsruhe
- Aufsatz zum Jones Day-Urteil: Internal Investigations sind anwaltliche Tätigkeit

Diese Themen sowie unser Newsletterarchiv finden Sie unter **news.wirtschaftsstrafrecht.de.**

tungsbedürftig sind. Hierbei könne zwar der Schutz von Informanten ein an sich anerkennenswertes Geheimhaltungsinteresse darstellen. Allerdings sei stets eine auf den konkreten Umständen des Einzelfalls beruhende Güterabwägung zwischen dem arbeitgeberseitigen Geheimhaltungsinteresse einerseits und dem arbeitnehmerseitigen Auskunftsinteresse andererseits vorzunehmen. Für das Vorliegen von Geheimhaltungsinteressen sei der Arbeitgeber zudem darlegungspflichtig. Dem werde der Arbeitgeber nicht gerecht, wenn er sich lediglich pauschal auf das Bestehen eines Geheimhaltungsinteresses ohne weitere Substantiierung beruft. Soweit das Unternehmen den Hinweisgebern Anonymität zugesichert habe, dürften Informationen, die Rückschlüsse auf die Person des Hinweisgebers zulassen nicht zur Akte genommen oder geschwärzt werden.

Dies bedeutet: Gelangen entsprechende Informationen über die Identität eines Whistleblowers zur (Personal-)Akte bzw. zum Vorgang, sind sie dem Betroffenen zu offenbaren.

Für Unternehmen die ein Whistleblowingsystem betreiben bedeutet dies, dass sie ihren Mitarbeitern bei Nutzung des Systems nur dann Anonymität zusichern können, wenn sie dafür sorgen, dass der Name des Meldenden nicht zur Akte gelangt. Anderenfalls muss die Identität des Meldenden gegenüber dem Betroffenen offenbart werden. Noch weiter geht die Datenschutzkonferenz des Bundes und der Länder, die dem Betroffenen in jedem Fall einen Anspruch zubilligt, die Identität des Whistleblowers zu erfahren, was die Bereitschaft zu unternehmensinternen Meldungen erheblich senken dürfte.

2. Konflikt zwischen EU Whistleblower-Richtlinie und Datenschutz

Eines der Kernelemente der Whistelblower-Richtlinie ist die Gewährung von Anonymität für den Whistleblower, was in Konflikt zu den Vorgaben der DSGVO steht. Dieser ist durch die EU zunächst übersehen worden. Im Rahmen der Überarbeitung der Whistleblower-Richtlinie ist nunmehr bestimmt worden, dass die Wirksamkeit der Whistleblower-Richtlinie unbedingt durchgesetzt werden soll und die Mitgliedstaaten hierfür auch die Datenschutzrechte der betroffenen Personen gemäß Art. 23 DSGVO einschränken können, soweit dies erforderlich ist, um einer Behinderung oder Verlangsamung der Meldung entgegenzutreten und die Meldung zu verfolgen.

Bis zur Umsetzung der Richtlinie in nationales Recht sollten Unternehmen daher erwägen, Meldungen entweder anonym entgegenzunehmen oder jedenfalls die Klarnamen der Hinweisgeber nicht in den Aktenvorgang zu übernehmen.

Praktische Auswirkungen?

VBB Praxisforum

Am 26.04.2019 ist das Geschäftsgeheimnisgesetz nach langen Verhandlungen – und mit einem Jahr Verspätung – in Kraft getreten. Für Unternehmensjuristen gilt: Jetzt fängt die Arbeit erst an!

Auf unserem **VBB Praxisforum am 11.07.2019** werden wir gemeinsam mit Experten aus dem Gesetzgebungsverfahren,

Herrn **Ingmar Jung**, Mitglied des Deutschen Bundestages, Mitglied im Ausschuss für Recht und Verbraucherschutz sowie Berichterstatter der CDU/CSU-Fraktion für den Gewerblichen Rechtschutz,

und aus den Wirtschaftsverbänden,

Frau **Doris Möller**, Deutscher Industrie- und Handelskammertag, Referatsleiterin Recht des Geistigen Eigentums, Recht in der digitalen Gesellschaft,

diskutieren, welche Herausforderungen jetzt auf Unternehmen zukommen, wo Gefahren lauern und wie Unternehmen ihre Geheimnisse wirksam schützen können.

- Wann? Donnerstag, 11.07.2019 von 14:30 Uhr bis 18:00 Uhr mit anschließendem „get together"

- Wo? INNSIDE Düsseldorf Hafen Speditionstrasse 9

Anmeldung im Internet unter www.wirtschaftsstrafrecht.de/praxisforum.php per E-Mail unter **praxisforum@wirtschaftsstrafecht.de** oder telefonisch unter 0211 36 777 0.

Wir freuen uns über Ihre **Zusage bis zum 28.06.2019.**

Die offizielle Einladung finden Sie unter www.wirtschaftsstrafrecht.de

Impressum

V.i.S.d.P.: RA Sven Diener (Schriftleitung)
Hrsg.: VBB Rechtsanwälte
Königsallee 74, 40212 Düsseldorf
Tel. +49 (0) 211 - 36 777 0
Fax +49 (0) 211 - 36 777 36
news@wirtschaftsstrafrecht.de
Newsletter abbestellen, Adresse ändern?
Eine Nachricht per Fax oder per E-Mail genügt.
Haftungsausschluss: Dieser Newsletter ersetzt keine rechtliche Beratung im Einzelfall. Für die Richtigkeit und Vollständigkeit kann trotz sorgfältiger Recherche keine Haftung übernommen werden.