Board Office Biedenbach

Frankfurt School of Finance & Management
German Excellence. Global Relevance.

THEMA:
WAS MÜSSEN UNTERNEHMEN TUN, DAMIT GESCHÄFTSGEHEIMNISSE AUCH GESCHÄFTSGEHEIMNISSE BLEIBEN?

***Referent: Dr. Jan Ehling** (Rechtsanwalt und Partner der Kanzlei AGS Legal, Frankfurt am Main).*

EXECUTIVE SUMMARY

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ist im April 2019 in Kraft getreten. Aufgrund der hohen Aufmerksamkeit, die die Unternehmen der Datenschutzgrundverordnung aus 2018 widmeten (insbesondere ihrer umfangreichen Umsetzung), rückte die Umsetzung des neuen Geschäftsgeheimnisgesetzes in den Hintergrund. Das Gesetz sieht vor, dass nur wenn Unternehmen angemessene Geheimhaltungsmaßnahmen treffen, ihre Geschäftsgeheimnisse künftig auch durch das neue Gesetz geschützt sind. Somit ist vor allem der Vorstand, aber auch der Aufsichtsrat im Rahmen seiner Compliance-Verantwortung angehalten, sich mit diesem Thema zu befassen.

WESENTLICHE INHALTE DES VORTRAGS

Nach der bisherigen Rechtslage lag ein vom Gesetz geschütztes Geschäftsgeheimnis vor, wenn, vereinfacht gesagt, ein **manifestierter Geheimhaltungswille** bestand und der Sinn und Zweck der Geheimhaltung erkennbar war. Nunmehr wird ein Geschäftsgeheimnis anhand folgender Kriterien definiert:

- Die Information darf nicht allgemein bekannt sein.
- Das Geheimnis hat einen wirtschaftlichen Wert und ein Verlust wäre mit negativen Folgen für den Geschäftsinhaber verbunden.
- Es besteht ein berechtigtes Interesse an der Geheimhaltung.

Zusätzlich sieht das Gesetz vor, dass **angemessene Maßnahmen zur Geheimhaltung** getroffen worden sind und ordnet die Beweislast dem Geschädigten zu.

Das Gesetz regelt auch Ausnahmen, bei deren Vorliegen die Erlangung, Nutzung oder Offenlegung eines Geschäftsgeheimnisses nicht verboten ist. So sieht es z.B. vor, dass Hinweisgeber („**Whistleblower**") keine Konsequenzen zu fürchten haben, wenn die Preisgabe des Geschäftsgeheimnisses „zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens" erfolgt und dies geeignet ist, das allgemeine öffentliche Interesse zu schützen. Allerdings muss der Whistleblower bei einer fehlerhaften Einschätzung bzw. unwahren Offenlegung eines Geschäftsgeheimnisses damit rechnen, dem Geheimnisinhaber Schadenersatz für dessen materiellen und immateriellen Schaden leisten zu müssen.

Es lohnt einen genaueren Blick auf die Definition der angemessenen Maßnahme zu werfen. Angemessenheit ist u.a. nach dem Wert des Geheimnisses zu beurteilen und auch unternehmensspezifische Kriterien (wie Größe oder Branchenüblichkeit) sind zu berücksichtigen. Neu ist zudem die Beweislast des Geschädigten. Hier gilt es eine Dokumentation zu erstellen, schon bevor der Fall eintritt. Handlungsverpflichteter ist in diesem Fall die Geschäftsführung bzw. der Vorstand (Haftungsrisiko: §93 AktG, 43 GmbHG).

KONKRETER HANDLUNGSBEDARF – SCHRITTWEISES VORGEHEN

Zunächst sollte definiert werden, welche Geschäftsgeheimnisse es im Unternehmen gibt. Diese sollten in Risikogruppen kategorisiert werden. Denkbar sind drei Kategorien, je nach potentiellem Schaden bei Verlust: „Überlebenswichtig", „Wichtig" „Sensibel". Die laufenden Maßnahmen sollten unbedingt dokumentiert und auf ihre Wirksamkeit und Angemessenheit immer wieder überprüft werden.

GRUNDSATZFRAGE: WER BENÖTIGT WELCHE INFORMATIONEN?

Zur Sicherstellung der Geheimhaltung können, je nach Einzelfall, folgende Maßnahmen ergriffen werden:

- Physische Maßnahmen:
- Zutritts- und Zugangskontrollen auf das Firmengelände
- Absicherung des Serverraums

- Abschließbare Schränke / Container
- Elektronische Maßnahmen:
- Berechtigungsmanagement
- Passwort-Richtlinien
- Backup / Archivierungsstrategien
- Firewalls
- 2-Faktor-Authentifizierung
- Verschlüsselung von Endgeräten
- Organisatorische Maßnahmen:
- Verantwortlichkeiten klar regeln
- Aufnahme des Themas Geschäftsgeheimnisse in die Compliance-Richtlinien
- Strukturierung Joiner – Leaver Prozess
- Clean Desk Richtlinie
- Awareness Schulungen
- Analyse von „Angriffswegen"
- Rechtliche Maßnahmen:
- Vertraulichkeitsvereinbarungen mit Vertragspartnern
- Vertragsstrafen implementieren
- Prüfen, inwieweit „one fits all" möglich ist, etwa in den AGBs
- Für sensible Vorgänge gesonderte NDAs verwenden

Arbeitsrechtliche Maßnahmen sind z.B. Geheimhaltungsvereinbarung im Arbeitsvertrag, ein nachvertraglicher Schutz und Absicherung gegen „Erfahrungswissen", projekt- oder einzelfallbezogene NDAs, Vertragsstrafenregelungen oder auch Betriebsvereinbarungen, die Geheimhaltungsvereinbarungen vorsehen können.

FRAGEN AN DEN REFERENTEN

In der anschließenden Q&A Session wurde u.a. diskutiert, welche Rolle der Aufsichtsrat in diesem Kontext spielt. Neben seiner Aufgabe in der Überwachung der Compliance, sind Aufsichtsräte zudem Empfänger und Sender von vertraulichen Informationen. Hier gilt es ebenfalls die nötigen Sicherheitsmaßnahmen an den Tag zu legen – insbesondere, wenn Aufsichtsräte z.B. nicht in die IT-Umgebung des Unternehmens eingebunden sind. Bei Mandaten in internationalen Unternehmen ist zu beachten, dass hier zumindest EU-weit vergleichbare Regelungen gelten. Über die EU hinaus setzt das Recht einen sehr hohen Standard. Ergänzend wird empfohlen, zu überprüfen, ob in anderen Ländern noch erweiterte Regelungen zu beachten sind. Bei der Frage der Herausgabe von Informationen an externe Stakeholder wie Rating-Agenturen empfiehlt der Referent hier eher restriktiver vorzugehen, um die Grenze zu Geschäftsgeheimnissen nicht zu verwässern und keine Risiken in Kauf zu nehmen.

Juni 2020