

Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung

1. Status quo

Bislang gab es unterschiedliche Ansätze zum Schutz von Geschäftsgeheimnissen in der Europäischen Union bzw. dem EWG. Dies wurden durch die Richtlinie (EU 2016/943) mit einer Umsetzungsfrist bis **09.06.2018** vollharmonisiert.

In Deutschland ist mangels bisheriger Umsetzung eine unmittelbare Anwendungswirkung zu bejahen. Der Schutz von Geschäftsgeheimnissen wird in Deutschland bisher durch das Gesetz gegen den unlauteren Wettbewerb (UWG) und das BGB geregelt. Letzter legislativer Bearbeitungsstand ist der Regierungsentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung vom 18.07.2018, welche im März 2019 vom Kabinett gebilligt wurde.

2. Avisierte Änderungen durch das GeschGehG-E

Warum bedarf es einer Regelung?

- Schutz von Geschäftsgeheimnissen kann weder den Marktverhaltensregelungen des UWG noch den vollständigen Immaterialgüterrechten wie zum Beispiel dem Patent- und Markenrecht zugeordnet werden.
- Unterschiede zu den Immaterialgüterrechten bestehen insofern, als der Schutz von Geschäftsgeheimnissen von der tatsächlichen Geheimhaltung der Information abhängt und keine besondere Qualität der Informationen für den rechtlichen Schutz erforderlich ist.
- Von den reinen Marktverhaltensregelungen des UWG unterscheidet sich der Schutz von Geschäftsgeheimnissen insofern, als er sich auf eine Information bezieht, die handelbar ist und regelmäßig wirtschaftlichen Wert besitzt.
- Unternehmen investieren in den Erwerb, die Entwicklung und die Anwendung von Know-How und Informationen — die Währung der wissensbasierten Wirtschaft, die einen Wettbewerbsvorteil schafft
- Unternehmen sind zunehmend unlauteren Praktiken ausgesetzt, die auf eine rechtswidrige Aneignung von Geschäftsgeheimnissen abzielen, wie Diebstahl, unbefugtes Kopieren, Wirtschaftsspionage oder Verletzung von Geheimhaltungspflichten.
- Es bedarf homogener und rechtsicherer Regelungen zur einheitlichen Begriffsdefinition, Inhaberschaft, zum Erwerb, Nutzung oder Offenlegung von Geschäftsgeheimnissen, prozessualen Darlegungen sowie von Sanktionen in Fällen unbefugter bzw. rechtswidriger Handlungen und/oder Unterlassungen

3. Besondere Änderungen durch das GeschGehG-E – Reverse Engineering

- Neuregelung in § 3 Absatz 1 Nr. 2 GeschGehG bzw. Art. 3 Absatz 1 lit. b) EU 2016/943!
- Ein Geschäftsgeheimnis darf insbesondere erlangt werden durch ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der

a) öffentlich verfügbar gemacht wurde oder

b) sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt;

- **Ist insofern keine Verpflichtung zur Geheimhaltung vorhanden, können Dritte durch ein legales Reverse Engineering selbstständig eigene Geschäftsgeheimnisse erlangen!**

4. Pflicht zum Vorhalten von angemessenen Schutzmaßnahmen

- Die Art der Geheimhaltungsmaßnahmen hängt von der Art des GeschGeh und den konkreten Umständen der Nutzung a.b
- Die Maßnahmen sind stets einzelfallabhängig
- Angemessenheit kann sich nach Wert des GeschGeh, Entwicklungskosten, Bedeutung für das Unternehmen, übliche Geheimhaltungsmaßnahmen im Unternehmen, Art der Informationskennzeichnung sowie vertraglichen Regelungen mit Auftragnehmern und Geschäftspartnern bemessen
- Bisher gibt es keine verlässliche Auslegungsrichtlinie für die Konkretisierung von angemessenen Geheimhaltungsmaßnahmen (aber Orientierung an Art. 32 DS-GVO).
- Empfehlenswert ist es, ein konkretes Schutzkonzept zu erarbeiten und womöglich in einer unternehmensinternen Richtlinie festzuhalten (neben bestehenden Datenschutz und IT-Sicherheitsdokumentation – inklusive einer turnusmäßigen Evaluation).

5. Verpflichtende Klassifizierung von Informationen

- Ein umfassendes Schutzkonzept bedingt eine Informationsklassifizierung.
- Nicht alle Informationen des Unternehmens sind auch GeschGeh -> Identifizierung von GeschGeh notwendig
- Bei fehlender Klassifizierung besteht das Risiko, dass alle Informationen gleichbehandelt werden, weshalb dann nicht mehr von Angemessenheit gesprochen werden kann
- Klassifizierung nach „öffentlich“, „intern“, „vertraulich“ und „streng vertraulich“ ist möglich

6. Vertragliche Mindestmaßnahmen:

- Technisch-organisatorische Maßnahmen (Erfassung der angemessenen Schutzmaßnahmen)
- Arbeitsrechtliche Maßnahmen (Sensibilisierung, ggf. gesonderte Mitarbeiterverpflichtung)
- Geheimhaltungsklauseln im konkreten Vertrag oder gesonderte Geheimhaltungsvereinbarung und konkretem Verbot des Reverse Engineering (NDA)
- Vertragsstrafen etc.