Handlungsbedarf für Unternehmen aufgrund des neuen Gesetzes zum Schutz von Geschäftsgeheimnissen

© Bild von Uboiz auf Pixabay

Am 26. April 2019 trat das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) in Kraft. Es setzt die sog. Geschäftsgeheimnis-Richtlinie oder Know-How-Schutz-Richtlinie ((EU) 2016/943, „Trade Secrets Directive") in deutsches Recht um. Ziel des GeschGehG ist, eine europaweit einheitliche zivilrechtliche Regelung zu schaffen, um Geschäftsgeheimnisse, die häufig den wesentlichen Vermögenswert eines Unternehmens darstellen, effektiv zu schützen. Bislang fand ein Geheimnisschutz im deutschen Recht insbesondere über die Vorschriften der §§ 17 ff. UWG statt, die mit Inkrafttreten der GeschGehG weggefallen sind.

Aufgrund der neuen Rechtslage genießt eine Information künftig nur noch dann den Schutz als Geschäftsgeheimnis, wenn nachweislich angemessene vertragliche, organisatorische und/oder technische Geheimhaltungsmaßnahmen getroffen worden sind. Das Gesetz stellt daher neue organisatorische Anforderungen an die Unternehmen, die sich auf Geschäftsgeheimnisschutz berufen möchten.

Geschäftsgeheimnis, § 2 GeschGehG

Die Vorschrift des § 2 GeschGehG definiert „Geschäftsgeheimnis" als

- 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 Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und
- daher von wirtschaftlichem Wert ist und
- die Gegenstand von angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
- bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Bei einem Geschäftsgeheimnis kann es sich sowohl um technisches als auch um kaufmännisches Wissen handeln.

Angemessene Geheimhaltungsmaßnahmen, § 2 Nr. 1 b GeschGehG

Wie beim Datenschutz können unterschiedliche Arten von Geheimhaltungsmaßnahmen getroffen werden, nämlich

- organisatorische Maßnahmen (Festlegung von Verantwortlichkeiten, Erstellung eines Schutzkonzepts etc.), inklusive personelle und kommunikative Maßnahmen (Mitarbeiterschulungen etc.)
- technische und physische Schutzvorrichtungen (Firewall, Safe, Passwortschutz etc.)
- rechtliche Maßnahmen (Vertraulichkeitsvereinbarungen etc.).

Einzelheiten sind in der im Info-Kasten dargestellten Checkliste aufgeführt.

Die Bewertung der „Angemessenheit" einer Geheimhaltungsmaßnahme erfolgt nicht nach starren Kategorien, sondern anhand einer einzelfallabhängigen Gesamtbetrachtung, insbesondere unter Berücksichtigung der folgenden Faktoren:

- Größe und Bedeutung des Unternehmens
- Wert der Information
- Entwicklungskosten
- Grad des Wettbewerbsvorteils durch die geheime Information
- möglicherweise bestehende Schwierigkeiten bei der Geheimhaltung
- konkrete Gefährdung der Information etc.

Erlaubte Handlungen, § 3 GeschGehG - Eigenständige Entdeckungen und Schöpfungen, Reverse Engineering, Sonderregelungen

Ein Geschäftsgeheimnis darf durch eine eigenständige Entdeckung oder Schöpfung (sog. Parallelentdeckung, Parallelschöpfung) erlangt werden. Im Falle einer Parallelentdeckung oder -schöpfung kann es also durchaus mehrere Inhaber desselben Geschäftsgeheimnisses geben.

Aufgrund der Neuregelung darf ein Geschäftsgeheimnis grundsätzlich auch durch Beobachten, Untersuchen und Rückbauen, sog. Reverse Engineering, oder Testen eines Produkts oder Gegenstands erlangt werden, sofern sich das Produkt oder der Gegenstand im rechtmäßigen Besitz des Beobachtenden, Untersuchenden oder Rückbau-

enden befindet und dieser keinen vertraglichen Beschränkungen unterliegt.

Die völlige Legalisierung des Reverse Engineerings ist eine einschneidende Neuerung im Vergleich zur bisher in Deutschland geltenden Rechtslage. Ausdrückliches Ziel des GeschGehG ist es, den technischen Fortschritt durch Produktbeobachtung und -rückbau zu fördern, allerdings nur bis zur Grenze bestehender gewerblicher Schutzrechte, wie Patent- oder Designrechte, die dadurch wohl noch mehr an Bedeutung gewinnen werden. Bislang war Reverse Engineering nach der Rechtsprechung nur dann zulässig, wenn jeder Fachmann ohne größeren Aufwand zur Ableitung in der Lage gewesen wäre, das Geschäftsgeheimnis also gewissermaßen „offenkundig" war.

Insbesondere im Umgang mit Prototypen und Musterstücken sollten Unternehmen daher in Zukunft sehr sorgfältig darauf achten, ob, wem und in welchem Umfang sie diese zur Verfügung stellen und die notwendige Geheimhaltung sowie das Verbot eines Reverse Engineerings auch vertraglich absichern.

Des Weiteren sieht § 3 GeschGehG vor, dass ein Geschäftsgeheimnis durch Gesetz, auf Grund eines Gesetzes oder Rechtsgeschäfts erlangt, genutzt oder offengelegt werden darf. Hierdurch wird klargestellt, dass Sonderregelungen in anderen Gesetzen vorgehen.

Handlungsverbote, § 4 GeschGehG

Die Handlungsverbote sind in § 4 GeschGehG aufgelistet. Ein Geschäftsgeheimnis darf insbesondere nicht erlangt werden durch unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder durch jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.

Ausnahmen, Schutz von Hinweisgebern, sog. „Whistleblowern", § 5 GeschGehG

Die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses fällt nicht unter die Verbote des § 4 GeschGehG, wenn dies zum Schutz eines berechtigten Interesses erfolgt, insbesondere

1. zur Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit, einschließlich der Achtung der Freiheit und der Pluralität der Medien;

2. zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen;

3. im Rahmen der Offenlegung durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn dies erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann.

Diese Voraussetzungen müssen objektiv gegeben sein. Der gute Wille des Hinweisgebers reicht nicht aus. Den gutgläubigen Hinweisgeber schützen jedoch die allgemeinen Irrtumsvorschriften.

Ansprüche bei Rechtsverletzungen, §§ 6 ff. GeschGehG

Das GeschGehG gibt dem Geheimnisinhaber verschiedene Ansprüche gegenüber dem Verletzer des Geschäftsgeheimnisses:

- Beseitigungs- und Unterlassungsanspruch bei drohender oder bereits eingetretener Rechtsverletzung, § 6 GeschGehG
- Recht auf Vernichtung, Herausgabe, Rückruf, Entfernung oder Rücknahme der rechtsverletzenden Produkte vom Markt, § 7 GeschGehG
- Auskunftsanspruch und Schadensersatzanspruch bei Verletzung der Auskunftspflicht, § 8 GeschGehG
- Schadensersatzanspruch, § 10 GeschGehG

Der vorsätzlich oder fahrlässig handelnde Verletzer hat dem Inhaber des Geschäftsgeheimnisses den entstandenen Schaden zu ersetzen. Hierbei kann der Schaden auch auf der Grundlage der Gewinnabschöpfung oder der Lizenzanalogie berechnet werden.

Verfahrensbesonderheiten, §§ 15 ff. GeschGehG

Für Geschäftsgeheimnisstreitsachen ist das Gericht ausschließlich zuständig, in dessen Bezirk der Beklagte seinen allgemeinen Gerichtsstand hat. Zwar sind die Länder ermächtigt, Geheimnisschutzgerichte zu bestimmen; es bleibt jedoch abzuwarten, ob dadurch ein effektiver Geheimnisschutz bewirkt werden kann.

Zwar sieht § 16 GeschGehG eine Geheimhaltungspflicht für die Gerichtsverfahren beteiligten Personen vor; diese dürfte aber in der Praxis nur bedingt hilfreich sein, da die Prozessparteien und möglicherweise auch sonstige am Verfahren beteiligte Personen den vollen Einblick in die Geschäftsgeheimnisse während eines Verfahrens erhalten.

Strafvorschriften, § 23 GeschGehG, §§ 201 ff. StGB

Die Verletzung eines Geschäftsgeheimnisses kann mit Freiheitsstrafe von bis zu 3 Jahren oder mit Geldstrafe bestraft werden, § 23 GeschGehG. Zu beachten ist jedoch, dass es sich um ein Antragsdelikt handelt, d.h., dass der Strafantrag innerhalb von 3 Monaten ab Kenntnis gestellt werden muss.

Des Weiteren gelten auch nach Inkrafttreten der GeschGehG insbesondere die folgenden allgemeinen Strafvorschriften:

- § 201 StGB Verletzung der Vertraulichkeit des Wortes
- § 202 StGB Verletzung des Briefgeheimnisses
- § 202 a StGB Ausspähen von Daten
- § 203 StGB Verletzung von Privatgeheimnissen
- § 204 StGB Verwertung fremder Geheimnisse
- § 206 StGB Verletzung des Post-und Fernmeldegeheimnisses

Angemessene Maßnahmen zum Geheimnisschutz - Checkliste

Jedes Unternehmen sollte daher prüfen, ob es ausreichend auf die Anforderungen des neuen Rechts vorbereitet ist. Ob angemessene Schutzmaßnahmen getroffen wurden, lässt sich nicht pauschal für alle Unternehmen bestimmen. Wie oben dargestellt, kommt es dabei auf eine Gesamtbetrachtung unter Berücksichtigung verschiedener Faktoren an. Von zentraler Bedeutung sind jedoch die sorgfältige Dokumentation und die Sicherstellung der zuverlässigen und dauerhaften Einhaltung der getroffenen technischen, organisatorischen und rechtlichen Maßnahmen.

Die Checkliste für angemessene Maßnahmen zum Geheimnisschutz nennt die aus Sicht der Verfasserin wichtigsten Punkte, erhebt jedoch keinen Anspruch auf Vollständigkeit.

Checkliste

für Maßnahmen zum Geheimnisschutz:

I. Organisatorische Maßnahmen

1. Festlegung eines Geheimnisschutzbeauftragten
2. Kennzeichnung und Klassifikation vorhandener Informationen als Geschäftsgeheimnis an Hand ihrer Bedeutung für das Geschäftsmodell und die Marktposition („Trade Secret Registry"),
   z.B. nach einem Dreistufenmodell in die Kategorien:
   - „Schlüssel-Know-how"
   - „Strategisch Wichtiges" und
   - „Sonstiges"
   und Anpassung des Aufwands für die jeweiligen Maßnahmen nach dem Wert des Geheimnisses für das Unternehmen
3. Schutzbedarfsanalyse, d.h. Ermittlung möglicher Risiken
4. Begrenzung des Informationszugangs nach dem „Need-To-Know"-Prinzip
5. Erstellung einer Geheimhaltungsrichtlinie
6. Regelungen für Besucher, z.B. Voranmeldung, Besucherausweise, Dokumentation der Teilnehmer bei Meetings, Umgang mit Mobiltelefonen, Abholung der Besucher durch Mitarbeiter, Verbot von Foto- und Videoaufnahmen, Kopien etc.
7. Aufstellung von Regeln und Dokumentationsmechanismen für den Zugang zu Geschäftsgeheimnissen (Listen, IT-Protokolle etc.)
8. Prüfung von arbeitsteiligen Prozessen auf Geheimnisschutz
9. Strikte Trennung von dienstlichen und privaten Devices (Telefon, Tablet, Computer), d.h. Vermeidung von „Bring your own Device"-Konstellationen
10. Beschränkung der mitgenommenen Dateien bei (Auslands-)Reisen auf das Erforderliche
11. Einrichtung einer unternehmensinternen „Whistleblower-Hotline" oder eines externen, zur Geheimhaltung verpflichteten Ansprechpartners für den Whistleblower, z.B. eines Vertrauensanwalts des Unternehmens, an den sich der „Whistleblower" zunächst wenden muss
12. Aufstellung eines Ablaufplans für Schutz und Rechtsdurchsetzung im Falle von Rechtsverletzungen
13. Regelmäßige Information und Schulung der Mitarbeiter, beginnend beim Abschluss des Arbeitsvertrags,
14. insbesondere Hinweis auf Konsequenzen, bspw. Kündigungsrecht, (gesetzliche) Geheimhaltungspflichten (z.B. § 79 BetrVG, § 24 ArbNErfG, § 203 f. StGB)
15. Dokumentation der Information und Schulung der Mitarbeiter, z.B. durch Abgabe einer Erklärung durch die Mitarbeiter
16. Sorgfältige Auswahl und regelmäßige Überprüfung der zugangsberechtigten Mitarbeiter (insbes. Praktikanten, Trainees, Mitarbeiter in Probezeit)
17. Einrichtung von Melde- und gegebenenfalls Vergütungssystemen für neue Geschäftsgeheimnisse (vgl. § 17 ArbNErfG)
18. Einrichtung und regelmäßige Kontrolle einer Clean-Desk-Policy
19. Notfallplan mit internen Berichtsketten bei erfolgtem oder drohendem Verlust von Geschäftsgeheimnissen
20. Systematische Kontrollen bei Beendigung des Arbeitsverhältnisses oder Wechsel des Arbeitsplatzes, z.B. vollständige Rückgabe der geschäftsgeheimnisrelevanten Systeme, z.B. Laptop, Handy
21. Durchführung von „Exit"-Gesprächen bei Beendigung

Rechtstexte:

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG):

https://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html

Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung:

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L0943

des Arbeitsverhältnisses oder Wechsel des Arbeitsplatzes, insbesondere zum Thema Umfang und Fortdauer des Geheimnisschutzes

II. Technische und physische Maßnahmen

1. Aufstellung und Umsetzung von Berechtigungskonzepten für die relevanten IT-Systeme
2. Absicherung des Betriebsgeländes, Trennung der Netzwerke insbesondere strikte Trennung des Netzwerks/Computern von fremden (Speicher-)Geräten
3. Sperrung des externen Zugriffs auf zentrale/sensible Server (Homeoffice)
4. räumliche Trennung kritischer Bereiche, z.B. deutliche Trennung der Forschungs- und Entwicklungsabteilung vom Besucherbereich mit deutlicher Kennzeichnung der relevanten Räume mit Zutrittsverboten
5. Einrichtung von Maßnahmen zur IT-Sicherheit, z.B. ISMS (engl. für „Managementsystem für Informationssicherheit“) nach ISO 27001
6. Werkschutzmaßnahmen, z.B. durch Sicherheitspersonal, Zugangskarten etc.
7. Verschlüsselung von Kommunikation, z.B. von Internetverbindungen, E-Mails, Dokumenten etc.

III. Rechtliche Maßnahmen

1. Überprüfung und gegebenenfalls Ergänzung der Arbeitsverträge und der Verträge mit freien Mitarbeitern und Subunternehmern im Hinblick auf angemessene Verschwiegenheitsklauseln
2. Nachweis der Kenntnis der Mitarbeiter über die Qualifikation als Geheimnis (Wissenserklärung des Mitarbeiters)
3. Erstellung bzw. Überprüfung und Ergänzung von internen Richtlinien mit Hinweisen auf die die Geheimhaltungspflichten in Arbeitsverträgen, Betriebsvereinbarungen, ArbNErfG, § 242 BGB etc.
4. Begrenzung des Informationszugangs und der Informationsweitergabe durch interne Anweisungen (Vertraulichkeitsvereinbarung als Voraussetzung für Informationsweitergabe)
5. Überprüfung und gegebenenfalls Ergänzung der Verträge mit Dienstleistern, Kunden und Kooperationspartnern im Hinblick auf angemessene Verschwiegenheitsklauseln und Verbot von Reverse Engineering, insbesondere bei Lizenznehmern und Zulieferern
6. Erstellung bzw. Überprüfung und Ergänzung von Vertraulichkeitsvereinbarungen (NDA) in geheimnisschutzrelevanten Prozessen, z.B. bei F&E-Kooperationsverträgen, Entwicklungsaufträgen an externe Unternehmen, mit Vereinbarung über Vertragsstrafe, anwendbares Recht und Gerichtsstand/Schiedsklausel und
7. Überwachung von deren Einhaltung
8. Vorbereitungen zur unverzüglichen Rechtsdurchsetzung bei Verletzungen, z.B. Erstellung eines Notfallplans, Festlegung des zu beauftragenden Rechtsanwalts, Vorbereitung der notwendigen Dokumente für eine zeitnahe Klageerhebung als Geheimnisschutzstreitsache

■ *Rechtsanwältin Gabriele Freifrau v. Thüngen-Reichenbach*

Rechtsanwältin Gabriele Freifrau von Thüngen-Reichenbach ist Fachanwältin für gewerblichen Rechtschutz, für Urheber- und Medienrecht und für IT-Recht sowie Zertifizierte Datenschutzbeauftragte (TÜV -Süd) in Coburg/Bayern. Sie berät und unterstützt Unternehmen und Selbständige bei der Vertragsgestaltung, der rechtskonformen Gestaltung ihrer Webseiten, der Entwicklung und Umsetzung umfassender Schutzrechts-Strategien für geistiges Eigentum (Marken und Designs), sowie bei der Umsetzung gesetzlicher Regelungen, z.B. Datenschutz und Wettbewerbsrecht, insbesondere in der digitalen Welt und ist auch als externe Datenschutzbeauftragte und Geheimnisschutzbeauftragte für mittelständische Unternehmen tätig.

www.von-thuengen.de