CHECKLISTE

Der Mittelstand. BVMW
Bundesverband mittelständische Wirtschaft
Unternehmerverband Deutschlands e.V.

10 TIPPS ZUR UMSETZUNG DES GESCHÄFTSGEHEIMNISGESETZES

DAS GESETZ IN KÜRZE:

Am 26.04.2019 ist das Geschäftsgeheimnisgesetz (GeschGehG) in Kraft getreten. Dies betrifft jedes Unternehmen, das über Informationen verfügt, die vor dem unbefugten Zugriff durch Dritte geschützt sein sollen. An diesen Schutz stellt das neue Gesetz nunmehr neue und erheblich höhere Anforderungen. Bisher wurden geheime Informationen fast immer automatisch als Geschäftsgeheimnisse angesehen und vor Missbrauch geschützt. Fortan muss der Geheimnisinhaber nachweisen, dass die Information **„Gegenstand von den Umständen nach angemessener Geheimhaltungsmaßnahmen"** ist. Für Unternehmen besteht somit das erhebliche Risiko, dass ihre Geheimnisse rechtlich nicht geschützt sind, weil bisher keine Maßnahmen ergriffen wurden oder diese Maßnahmen den neuen Anforderungen nicht genügen.

Das Gesetz bringt auch eine **verschärfte Produzentenhaftung** mit sich und es hebt das Verbot des **„Reverse Engineering"** weitgehend auf. Es sind keine konkreten Vorgaben enthalten, die klären, welche Maßnahmen zu ergreifen sind. Fest steht jedoch, dass Unternehmen tätig werden müssen. Die Umsetzung der Sicherheitsmaßnahmen ist dabei eine Organisationsaufgabe. Die Erstellung der Schutzkonzepte und die Umsetzung der Schutzmaßnahmen stellen Unternehmen vor große Herausforderungen.

Die folgenden Punkte sollen Ihnen eine Hilfestellung bei der Einrichtung eines Geheimnisschutzkonzeptes geben.*

1. Bestimmen Sie eine Person, die im Unternehmen für den Geheimnisschutz zuständig ist.

Diese Person ist zuständig für die Einrichtung eines ganzheitlichen und gerichtsfesten **Sicherheitsmanagementsystems** und organisiert den Geheimnisschutz. Sie hat die erforderlichen Befugnisse und auch einen Vertreter. Sie sollte mit Leitern der Abteilungen Entwicklung, IT, Marketing, Einkauf, Vertrieb, Buchhaltung und vor allem Personal kooperieren.

2. Identifizieren Sie schützenswerte Informationen im Unternehmen.

Als Geschäftsgeheimnisse kommen technische Informationen (z. B. Erfindungen, Konstruktionspläne, Formeln) und kaufmännische Informationen (z. B. Preislisten, Konditionen, Finanzdaten) in Betracht. Fertigen Sie eine **„Landkarte" der schützenswerten Informationen** an und ermitteln Sie, wo sie entstehen oder ins Unternehmen gelangen, wo sie gespeichert werden und wie sie im Unternehmen verteilt werden. Sortieren Sie die Informationen den Kategorien entsprechend und nutzen Sie dazu ein Dokumentationssystem.

3. Prüfen Sie, ob für die identifizierten schützenswerten Informationen Schutzrechtsanmeldungen in Betracht kommen.

Manche Erfindungen können besser durch Geheimhaltung geschützt werden, als durch Patentanmeldungen (z. B. Rezepte oder Verfahren, die nicht durch die Analyse des Produkts ermittelt werden können). In anderen Fällen ist ein **Patentschutz** besser. Dies sollte mit einem Patentanwalt erörtert werden. Bis zur Entscheidung ist die Geheimhaltung Pflicht.

Stand: September 2019

Der Mittelstand. BVMW
Bundesverband mittelständische Wirtschaft
Unternehmerverband Deutschlands e.V.

4. Teilen Sie das identifizierte schützenswerte Wissen in Kategorien ein.

Informationen, deren Verlust existenzgefährdend ist („Kronjuwelen“) sind der höchsten **Kategorie A** zuzuordnen. Strategisch besonders wichtiges Wissen, dessen Verlust erheblich spürbar ist, kann in **Kategorie B** eingeordnet werden. Sonstiges wettbewerbsrelevantes Wissen, dessen Verlust ärgerlich, aber verkraftbar ist, kann in **Kategorie C** eingeordnet werden. Nutzen Sie auch dazu ein Dokumentationssystem.

5. Legen Sie Schutzmaßnahmen fest.

Erstellen Sie ein **ganzheitliches, nachhaltiges und gerichtsfestes Sicherheitskonzept.** Die Maßnahmen müssen den Umständen entsprechend angemessen sein: Kategorie A erfordert die denkbar strengsten Sicherheitsmaßnahmen, Kategorie B erfordert strenge Maßnahmen, aber nicht auf dem allerhöchsten Niveau, Kategorie C erfordert wirksame, aber auch handhabbare Maßnahmen. Alle denkbaren technisch-organisatorischen und vertraglichen Maßnahmen können kombiniert werden. Sinnvoll ist eine Abwägung zwischen Kosten, Nutzen und Machbarkeit einerseits und Größe des Unternehmens und Bedeutung des Geheimnisses für das Unternehmen andererseits. Führen Sie eine **Risikoabschätzung** durch. Erwägen Sie, im Rahmen einer Wertbeitragsermittlung den Beitrag zum Unternehmenserfolg zu belegen und die erforderlichen Sicherheitsmaßnahmen zu begründen.

6. Implementieren Sie die festgelegten Schutzmaßnahmen.

Maßnahmen sind erforderlich im Verhältnis zu Arbeitnehmern und Geschäftspartnern sowie unbekannten Dritten („Betriebsspionage“). Insbesondere gegenüber Mitarbeitern ist das **„need-to-know-Prinzip“** zu beachten: Nur wer bei seiner Arbeit Zugang zu den Geheimnissen benötigt, erhält diesen Zugang (räumliche Trennung, Zugangsregelung für Räume und Behältnisse, Schließsysteme mit unterschiedlichen Berechtigungen, Verschlüsselung, Passwortregelung, Digital Rights Management, Kennzeichnung über Metadaten usw.). Wenn der Zugang zu Geschäftsgeheimnissen unvermeidlich ist, muss festgelegt werden, wie der Empfänger damit umzugehen hat, was er darf und was er nicht darf. Das darf nicht nur allgemein und pauschal erfolgen (keine „catch-all“-Klausel). Die Maßnahmen müssen dem konkreten Geheimnis angemessen sein. Achten Sie besonders auf das integrale Zusammenwirken der **baulichen, technischen und organisatorischen Maßnahmen.** Denken Sie dabei daran: **Weniger ist oft mehr.**

7. Dokumentieren Sie präventive und reaktive Schutzmaßnahmen.

Der Geheimnisinhaber muss im Streitfall beweisen, dass er **„den Umständen nach angemessene Geheimhaltungsmaßnahmen“** ergriffen hat. Damit die Maßnahmen jederzeit „angemessen“ sind, sollten die Schutzmaßnahmen dementsprechend regelmäßig überprüft und eventuell angepasst werden. Dokumentieren Sie den Umgang mit Informationen **eindeutig, nachvollziehbar** und **gerichtsfest** (Zugang, Zugriff, wer, was, wann, wo und wie):

a) Beschreiben Sie das Projekt hinsichtlich seines Umfangs und Inhalts zur rechtskonformen Umsetzung des neuen Gesetzes.
b) Legen Sie eine Liste mit den klassifizierten Geschäftsgeheimnissen entsprechend den neuen Begriffsbestimmungen an.
c) Belegen Sie die Entwicklung eines oder besser mehrerer Maßnahmenkataloge für die Umsetzung als Schutzkonzept.
d) Beweisen Sie mit Prüfberichten die tatsächliche Umsetzung der Schutzmaßnahmen.
e) Schaffen Sie ein ausreichendes Volumen an forensisch verwertbarem Datenmaterial über Insiderwissen von internen und externen Geschäftsgeheimnisträgern.
f) Fertigen Sie Protokolle über sämtliche Vertragsanpassungen mit internen und externen Trägern von Geschäftsgeheimnissen an.
g) Sichern Sie stets weiteres zweckbestimmtes Beweismaterial.
h) Denken Sie auch an die Sicherung des Materials für Mitarbeiterschulungen.

8. Führen Sie Schulungen durch und schaffen Sie ein Bewusstsein.

Sensibilisieren Sie die Arbeitnehmer in Bezug auf ihren täglichen Umgang mit sensiblen Informationen. Ziel ist die Schaffung von Vertrauen sowie eines Gespürs und eines Klimas der bewussten Geheimhaltung über regelmäßige Schulungen, Richtlinien, Regelwerke, ausführliche Verträge, Kontrollen der Regeln und Verträge, Sanktionen, Wahrnehmung des Weisungsrechts sowie Kommunikation des Geheimnisschutzes.

9. Vermeiden Sie die Infizierung mit fremden geschützten Geheimnissen.

Bei der **Einstellung neuer Mitarbeiter** oder bei neuen **Kooperationen** fließt schnell geheimes Wissen fremder Unternehmen in das eigene Unternehmen ein. Handelt es sich um fremde Geschäftsgeheimnisse, muss geklärt sein, dass sie benutzt werden dürfen. Ansonsten haftet das Unternehmen dem Geheimnisinhaber, und zwar teilweise auch dann, wenn der Umstand, dass es ein fremdes Geheimnis war, der Geschäftsleitung nicht bekannt war.

10. Überprüfen, aktualisieren und wiederholen Sie die Punkte 1. bis 9. regelmäßig.

Denken Sie daran: Sicherheit ist kein Zustand, sondern ein Prozess. Damit die Geheimhaltungsmaßnahmen jederzeit angemessen sind, sollte der Schutz regelmäßig überprüft und angepasst werden.

*Die Checkliste wurde mithilfe der BVMW Unternehmerkommissionen Recht sowie Unternehmenssicherheit nach bestem Wissen und mit größter Sorgfalt zusammengestellt. Diese Ausarbeitung ist nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen der BVMW bzw. die Autoren nicht. Die im vorliegenden Dokument gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen von der verantwortlichen Stelle für die jeweilige Situation im Unternehmen anhand der geltenden Vorschriften geprüft und angepasst werden.

Stand: September 2019

Der BVMW vertritt im Rahmen der Mittelstandsallianz über 900.000 Mitglieder. Die mehr als 300 Repräsentanten des Verbandes haben jährlich rund 800.000 direkte Unternehmerkontakte. Der BVMW organisiert mehr als 2.000 Veranstaltungen pro Jahr.

Kontakt:
Bundesverband mittelständische Wirtschaft (BVMW) e. V.
Bereich Volkswirtschaft & Politik
Potsdamer Straße 7, 10785 Berlin
Tel.: +49 (0)30 533206-0, Fax: +49 (0)30 533206-50
politik@bvmw.de; @BVMWeV; www.bvmw.de