DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

AdOrga Solutions

Gesetz zum Schutz von Geschäftsgeheimnissen

Geschäftsgeheimnisgesetz (GeschGehG)

Autoren:
Regina Mühlich
Dr. Jens Eckhardt

Stand: Mai 2020

Inhaltsverzeichnis

1 Einleitung

Das Gesetz zum Schutz von Geschäftsgeheimnissen („Geschäftsgeheimnisgesetz“) ist am 26. April 2019 in Kraft getreten.

Mit der am 08. Juni 2016 verabschiedeten Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 08. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABI. L 157 vom 15.06.2016, S. 1, waren die Mitgliedsstatten der Europäischen Union verpflichtet Regelungen zum Schutz von Geschäftsgeheimnissen umzusetzen. Im Gegensatz zu einer Grundverordnung, wie z. B. der Datenschutz-Grundverordnung (DS-GVO), welche unmittelbar und direkt gilt, ist eine Richtlinie in nationales Recht umzusetzen. Die Mitgliedsstaaten hatten hierzu zwei Jahre Zeit.

Bisher regelten die §§ 17 ff. UWG (Gesetz gegen unlauteren Wettbewerb) in Deutschland den Schutz von Betriebs- und Geschäftsgeheimnissen.

Das Ziel des Gesetzes ist in der Richtlinie wie folgt definiert: *„This directive lays down rules on the protection against the unlawful acquisition, use and disclosure of trade secrets.”*

2 Compliance

2.1 Regelkonformität

„Verhalten im Einklang mit geltendem Recht“ – das ist eine der gängigen Beschreibungen von Compliance. Compliance bedeutet allerdings mehr, nämlich den Grad der Einhaltung von Regeln **(Regelkonformität)**. Wer „compliant“ (engl. für übereinstimmend) ist, hält sich nicht nur an Recht, Gesetz und Ordnung, sondern idealerweise auch an die Leitlinien und das Wertesystem der eigenen Organisation.

Der Begriff Compliance ist noch relativ jung in seiner Verwendung für die Rechtstreue von Unternehmen und Betrieben. Eine Selbstverständlichkeit ist es allerdings, dass Unternehmen Gesetze einhalten müssen. Vorstände und Geschäftsführer haben die Sorgfalt eines ordnungsgemäßen Geschäftsleiters anzuwenden (§ 93 Abs. 1 AktG, § 43 Abs. 1 GmbHG). Dies bedeutet nichts anderes, als dass sie dafür Sorge tragen müssen, dass das Unternehmen die geltenden Gesetze einhält.

Die Besonderheit von Compliance im Kontext der Haftung der Unternehmensleitung besteht darin, dass sie nicht für einfache fehlerhafte Handlungen oder Unterlassungen haftet, sondern auch für die Nicht-Organisation der Einhaltung rechtlicher Vorgaben. Der alte Ansatz „alles gut, solange die Unternehmensleitung ihre Kenntnis abstreiten kann“ gilt gerade nicht mehr.

Überspitzt lässt sich das so umschreiben: Die Unternehmensleitung haftet, weil sie von der Rechtswidrigkeit wusste oder weil sie es nicht wusste, aber keine Maßnahme zur Verhinderung ergriffen hatte.

2.2 Herangehensweise

Alter Wein in neuen Schläuchen? Die erwähnten Paragraphen des Aktiengesetzes (AktG) und dem Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) sind schließlich nicht neu. Nicht ganz. Neu ist die Herangehensweise, die Aufgabe „compliant“ zu werden und zu sein. Es bedarf ein „Managementsystem“ – vor allem vor dem Hintergrund der sich ändernden Gesetze, wie beispielsweise die Änderung im Datenschutzrecht mit der Datenschutz-Grundverordnung (DS-GVO) im Mai 2018 oder das neue Geschäftsgeheimnisgesetz (GeschGehG) im April 2019.

Die rechtlichen Risiken nehmen also zu durch:

- dynamische Änderung des regulatorischen Umfelds auf internationaler und nationaler Ebene;
- extra-territoriale Wirkung ausländischer Normen (z. B. FCPA, UK Bribery Act, Loi Sapin II);
- Ausweitung der Haftung von Unternehmen und Geschäftsleiter durch Gesetzgeber, Gerichte und Behörden.

Die **neue Herangehensweise** ist somit eine Antwort auf ein sich laufend veränderndes Umfeld. Die Strafvorschriften haben sich verschärft. Gerichte gehen viel härter gegen Wirtschaftskriminalität vor. Dies ist auch dem Umstand geschuldet, dass Medien und die Öffentlichkeit von z.B. Korruption und Vorteilsnahme viel stärker Notiz nehmen als noch vor ein paar Jahren.

2.3 Unternehmerisches Handeln ist stets mit Risiko verbunden

Ob neue Produkte erfolgreich am Markt bestehen können, ob sich Investitionsentscheidungen letztlich auszahlen oder wie sich externe Rahmenbedingungen entwickeln, vieles hängt von einer bewussten Inkaufnahme bestimmter Risiken durch die Unternehmensleitung ab, ohne die erfolgreiches Wirtschaften nicht möglich wäre. [1]

Waren Buffet sagte „It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you’ll do things differently.” Ein Auf- und Ausbau eines Compliance-Systems ist für Unternehmen heute unerlässlich – um Risiken zu erkennen, zu minimieren und um vorzubeugen.

Im Compliance geht es aber um viel mehr als „nur“ um die Einhaltung von Gesetzen, die Minimierung von Risiken und die Vermeidung von Gesetzesverstößen. Sie beinhaltet neben verpflichtenden Regeln auch solche, denen sich eine Unternehmung freiwillig unterwirft, wie z. B. ISO-Standards, Verhaltensregeln oder Verhaltenskodex (Code of Contact).

[1] Vgl. Erste Hilfe zum GeschGehG, 2019, C.H.Beck Verlag

2.4 Konsequenzen für die Unternehmensleitung

Der Schutz von Geschäftsgeheimnissen als Wert („Asset“) eines Unternehmens ist eine zentrale Pflicht der Unternehmensleitung.

Eine Neuerung des GeschGehG wirkt sich hier aus: Früher waren nach § 17 UWG (gilt nicht mehr) Informationen bereits dann geschützt, wenn sie Betriebs- und Geschäftsgeheimnisse waren. Nach dem GeschGehG genügt allein die Einordnung als Betriebs- und Geschäftsgeheimnis nicht mehr, sondern der Schutz besteht nur, wenn auch Geheimhaltungsmaßnahmen ergriffen wurden.

Die Compliance zwingt die Unternehmensleitung daher dazu technische und/oder organisatorische Maßnahmen zu ergreifen, um die Geheimhaltung sicherzustellen.

Das allein genügt jedoch nicht. Dieser Schutz muss so dokumentiert sein, damit er in einer sog. Geheimnisschutzstreitsache auch objektiv nachvollziehbar dargelegt werden kann.

Das Aufsetzen und Implementieren technisch-organisatorischer Maßnahmen ist auch die „Brandschutztür“ einer persönlichen Haftung der Unternehmensleitung.

3 Das Geschäftsgeheimnis

§ 1 GeschGehG regelt den **Anwendungsbereich**. In Abs. 1 heißt es: „*Dieses Gesetz dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung.“*

Die Definition des Geheimnisses ist in vier Punkte aufgeteilt. Um die Definition des Geschäftsgeheimnisses zu erfüllen, müssen alle vier Voraussetzungen vorliegen:

Gemäß § 2 Nr. 1 GeschGehG ist ein Geschäftsgeheimnis eine[2]

1. eine Information, die weder insgesamt noch in genauer 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
2. von wirtschaftlichem Wert ist und
3. Gegenstand von – den Umständen nach angemessenen – Geheimhaltungsmaßnahmen durch den rechtmäßigen Inhaber ist und
4. bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Das Geschäftsgeheimnis beinhaltet die Vorgänge innerhalb eines Unternehmens, die nicht der Öffentlichkeit zugänglich gemacht werden sollen. Diese sind nur bestimmten Mitarbeitern innerhalb eines Unternehmens bekannt und unterliegen der absoluten

[2] Vgl. https://www.adorgasolutions.de/geschaeftsgeheimnisgesetz-geschgehg-verabschiedet/

Verschwiegenheitspflicht. Der Inhaber eines Betriebes hat an diesen Sachverhalten den absoluten Willen zur Geheimhaltung und dieser beruht auf einem wirtschaftlichen Interesse, das auch als besonders schutzwürdig deklariert ist.[3]

Laut dem GeschGehG ist ein Geschäftsgeheimnis 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.“*

Im Vergleich zur bisherigen Rechtslage in Deutschland, gelten dabei teilweise strengere Anforderungen an das Vorliegen eines Geschäftsgeheimnisses. So müssen Unternehmen zum Beispiel **angemessene Geheimhaltungsmaßnahmen** treffen, um von dem Schutz durch das Gesetz profitieren zu können. Die Einordnung als Geschäftsgeheimnis steht der Tätigkeit von Journalisten und Hinweisgebern jedoch nicht entgegen. Denn die Ausnahmeregelungen für Journalisten und Hinweisgeber gelten für sämtliche Geschäftsgeheimnisse.

Beispiele für Geschäftsgeheimnisse sind u. a.:

- Kunden-, Lieferantendaten und Adressverzeichnisse sowie XING-Kontakte;
- Angebote, Preiskalkulationen, Verhandlungstaktiken und Ausschreibungsunterlagen;
- Rezepte, Stoffzusammensetzungen, Materialbeschaffenheit und Beistoffe;
- Buchführungsunterlagen, Abschlüsse, Budget und (unveröffentlichte) Bilanzen;
- Computerprogramme, Software und Tools sowie Erfahrungen mit deren Umgang;
- Geschäftsstrategien, Forecasts, Unternehmensdaten und Planungen;
- Lohn- und Gehaltsdaten sowie geplanter Personalabbau und Förderungsprogramme;
- Telefondurchwahlnummern;
- Vorlagen und Vorschriften technische Art (unmittelbar aus § 23 GeschGehG) sowie Zeichnungen.

Neu – und über die EU-Richtlinie hinaus – fordert das deutsche GeschGehG auch ein berechtigtes Interesse an der Geheimhaltung. Auch dieses Interesse muss dokumentiert und im Rechtsstreit begründet werden können. Daher sollte dieses bereits gemeinsam mit den Schutzmaßnahmen dokumentiert werden.

[3] Vgl. https://www.adorgasolutions.de/geschaeftsgeheimnisgesetz-geschgehg-verabschiedet/

4 Angemessene Maßnahmen zur Geheimhaltung

Der Begriff der Maßnahme in der Gesetzesbegründung ist vielfältig auszulegen und ist nicht nur, aber auch, auf rechtliche Maßnahmen beschränkt. Neben

- **vertraglichen Geheimhaltungsmaßnahmen, die mehr oder weniger durchsetzbar sind,**

sind vor allem

- **organisatorische Maßnahmen**
- **technische Maßnahmen**

zum Schutz von Geschäftsgeheimnissen zu ergreifen, also mehr **präventiv** als Schadensbegrenzung.

Bei den vertraglichen Maßnahmen muss zwischen Angestellten, Freelancer und Kooperations- bzw. Vertragspartner unterschieden werden. Allgemein gefasste oder alles umfassende Verschwiegenheits- und Geheimhaltungsvereinbarungen sind hierbei typischerweise nicht zielführend. Vielmehr sind konkrete Vereinbarungen und Regelungen erforderlich. Das gilt auch für Auftragsverarbeiter. Wenngleich diese bereits nach Art. 28 DS-GVO zur Vertraulichkeit zu verpflichten sind, hat diese Vertraulichkeitsverpflichtung eine andere inhaltliche Ausrichtung.

Diese technischen und organisatorischen Maßnahmen sind aus dem Datenschutzrecht (z. B. Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO) bekannt. Dort geht es aber in erster Linie um den materiellen Datenschutz (Schutz des Rechtes auf informationelle Selbstbestimmung) und der Datensicherheit (z. B. Integrität, Vertraulichkeit, Verfügbarkeit).

Weitere Empfehlungen für die Umsetzung von technischen und organisatorischen Maßnahmen liefert das BSI IT-Grundschutz-Kompendium [4]

Hieraus können auch Maßnahmen zum Informationsschutz angewandt werden. Die technischen und organisatorischen Maßnahmen aus dem Datenschutz-Managementsystem sind auf jeden Fall eine sehr gute Grundlage und ein guter Ansatz für die im Rahmen des GeschGehG zu ergreifenden Maßnahmen:

- Zutrittskontrolle
- Zugriffskontrolle
- Zugangskontrolle
- Weitergabekontrolle
- Verfügbarkeitskontrolle
- etc.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 12.02.2020)

In Abhängigkeit der Branche und des Geschäftszweckes ist das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO ein guter Ausgangspunkt zur Erhebung der zu schützenden Informationen. Werden personenbezogenen Daten verarbeitet, kann man i.d.R. von einem Schutzbedarf auch im Rahmen des GeschGehG ausgehen.

Erkennen Sie die Parallelitäten zur DS-GVO. Nicht nur ist das Verzeichnis von Verarbeitungstätigkeiten eine gute Grundlage zur Identifikation von Schutzwürdigem, sondern auch der Schwachstellen. Das GeschGehG sieht auch keine konkreten inhaltlichen Vorgaben zur Bestimmung von „angemessenen Maßnahmen“ vor. Sie können sich an Art. 32 DS-GVO zur Bewertung orientieren. Sie müssen dabei aber den Unterschied im Schutzziel berücksichtigen und die Bewertung dementsprechend an einer anderen Zielrichtung ausrichten.

Denken Sie in Bezug auf diese Schutzpflichten weiter. Gerade in der aktuellen Diskussion um Homeoffice-Arbeit und Mobile Working muss auch der Schutz von Geschäftsgeheimnissen mitbedacht werden, um keine Schutzlücken zu riskieren.

5 Vorgehensweise

Die wichtigste Gesetzesänderung besteht wohl darin, dass Geschäftsgeheimnisse nur noch geschützt sind, wenn **angemessene Geheimhaltungsmaßnahmen getroffen** sind. In der Vergangenheit war es ausreichend, dass Geschäftsinformationen geheim bleiben sollten. Unternehmen müssen zukünftig ihre angemessenen Schutzmaßnahmen zur Geheimhaltung, damit Informationen auch weiterhin als Geschäftsgeheimnis Schutz genießen, **nachweisen** können. Es sind also auch aber nicht nur **interne Anweisungen und Richtlinien für Mitarbeiter** erforderlich. Vergleichbar mit der Nachweis- und Rechenschaftspflicht („Accountability“) aus Art. 5 Abs. 2 DS-GVO).

Welche Maßnahmen genau zu treffen sind, um nachweisen zu können, dass es sich um ein Geschäftsgeheimnis handelt, sagt das Gesetz leider nicht.

Allgemein kann gesagt werden:

- Unternehmen sollten idealerweise immer und überall Geheimhaltung vereinbaren. Unabhängig davon, ob es sich um eine Geschäftsanbahnung, eine Kooperation, Arbeitsverträge oder um Dienstleistungsverträge handelt.
- Technische Maßnahmen: Hier kann man sich u. a. am Datenschutz-Managementsystem orientieren wie z. B. Maßnahmen zur Zutritts-, Zugriffs- und Zugangskontrolle.
- Organisatorische Maßnahmen: Es sollte sichergestellt sein, dass nur Beschäftigte vertrauliche Informationen kennen und zu diesen Zugang haben, die für ihre Tätigkeit benötigt werden (u. a. Zugriffsmatrix, Berechtigungskonzept).

Die Implementierung des GeschGehG sollte wie auch die Einführung eines anderen Managementsystem z. B. im Datenschutz oder Qualitätsmanagement, angegangen werden. Auf jeden Fall ist ein strukturiertes Vorgehen erforderlich.

Praxistipp

Was ist ein Managementsystem?

Ein Managementsystem beschreibt Maßnahmen, die dazu beitragen, den Hauptzweck sowie die Rahmenbedingungen des Unternehmens sicher und effizient umzusetzen. Dazu erfasst das Managementsystem interne wie externe Anforderungen und setzt diese anschließend in Aufgaben um. Die Durchführung dieser Aufgaben wird organisiert und regelmäßig überprüft (PDCA-Zyklus). Entspricht sie nicht den festgelegten Kriterien, erfolgt eine Korrektur, die das System insgesamt verbessert und anpasst.

Der „Problemlösezyklus“ (Projektmanagement):

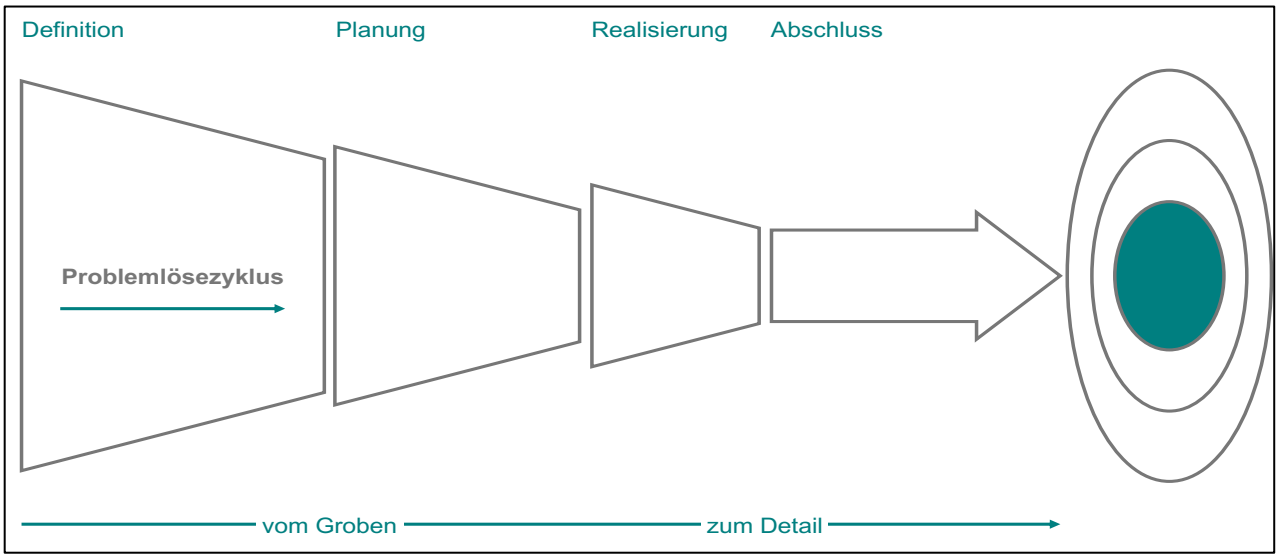


Abb. 1: Problemlösungszyklus (Quelle: Regina Mühlich, 2020)

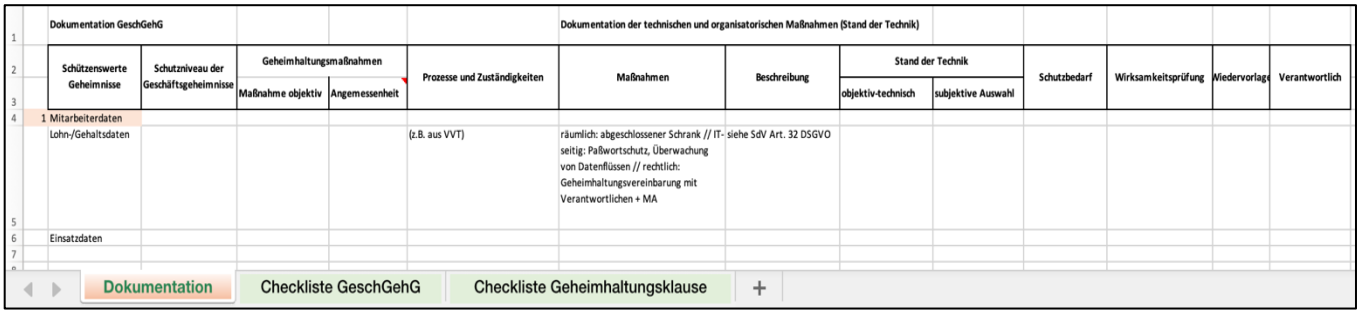
6 Handlungsempfehlungen

6.1 Erhebung – Informationen identifizieren [5]

Kategorie 1: Kritische Informationen (sog. Schlüsselinformationen)
Kategorie 2: Strategisch wichtige Informationen
Kategorie 3: Sonstige Informationen

[5] Landesamt für Verfassungsschutz Baden-Württemberg; eigene Darstellung

Beispiel:



Dokumentation GeschGehG					Dokumentation der technischen und organisatorischen Maßnahmen (Stand der Technik)						
Schützenswerte Geheimnisse	Schutzniveau der Geschäftsgeheimnisse	Geheimhaltungsmaßnahmen: Maßnahme objektiv	Geheimhaltungsmaßnahmen: Angemessenheit	Prozesse und Zuständigkeiten	Maßnahmen	Beschreibung	Stand der Technik: objektiv-technisch	Stand der Technik: subjektive Auswahl	Schutzbedarf	Wirksamkeitsprüfung	Wiedervorlage	Verantwortlich
1 Mitarbeiterdaten												
Lohn-/Gehaltsdaten				(z.B. aus VVT)	räumlich: abgeschlossener Schrank // IT-seitig: Paßwortschutz, Überwachung von Datenflüssen // rechtlich: Geheimhaltungsvereinbarung mit Verantwortlichen + MA	siehe SdV Art. 32 DSGVO						
Einsatzdaten												

Dokumentation | Checkliste GeschGehG | Checkliste Geheimhaltungsklause | +

Abb. 2: Erhebungsbogen (Quelle: Regina Mühlich, 2020)

6.2 Planung

Regelkreis des Managementsystems:

1. Planung
   Vorgaben: Gesetze (hier vorrangig das GeschGehG), Kunden, Lieferanten, etc.
2. Durchführung und Umsetzung
   Organisation, Prozessbeschreibungen, Anweisungen
3. Überprüfung
4. Anpassung

6.3 PDCA-Methode

Der PDCA-Zyklus, auch Deming-Zyklus genannt, beschreibt den vierstufigen Regelkreis des Kontinuierlichen Verbesserungsprozesses (KVP). Die Phasen sind: Plan, Do, Check, Act. Die Anwendung des Zyklus sorgt für einen kontinuierlichen und fortlaufenden (Verbesserungsprozess).

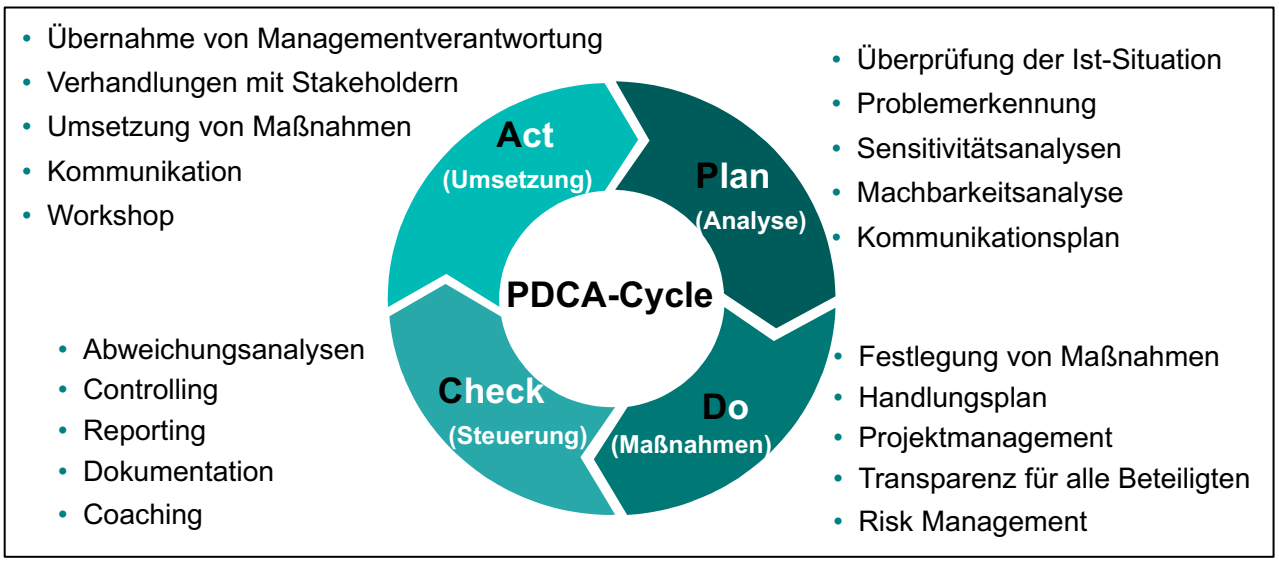


Abb. 3: PDCA-Methode (Quelle: Regina Mühlich, 2020)

6.4 Besonderes Augenmerk

6.4.1 Arbeitsverträge

Das Geschäftsgeheimnis hat ein weites arbeitsrechtliches Verständnis, welches wohl zukünftig eng i.S.v. § 2 Nr. 1 GeschGehG ausgelegt wird. Es ist daher empfehlenswert, die Klauseln entsprechend klarzustellen.

Derzeit (noch) typisch sind die so genannten „All-Klauseln“[6]:

> ***§ YX Verschwiegenheit, Aufbewahrung und Herausgabepflicht***
>
> *(1) Sowohl während der Dauer des Arbeitsvertrags als auch nach seiner Beendigung wird der Arbeitnehmer/die Arbeitnehmerin über alle ihm/ihr während der Vertragsdauer bekannt gewordenen geschäftlichen oder betrieblichen Angelegenheiten und Prozesse Stillschweigen bewahren und sämtliche ihm/ihr während der Vertragsdauer bekannt gewordenen Geschäftsgeheimnisse streng geheim halten. Diese betrifft insbesondere […Kundenlisten, Preislisten, Verträge, Bilanzen,…].*
> *(2) [Herausgabe Unterlagen]*

Bisher war ein Geheimnisschutzsystem nicht erforderlich, allgemeine Formulierungen (siehe oben) waren ausreichend.

Mögliche Formulierung der Klausel (Minimalklausel)[7]:

> ***„§ xy Verschwiegenheit, Schutz von Geschäftsgeheimnissen***
>
> *(1) Der Arbeitnehmer/die Arbeitnehmerin verpflichtet sich, alle Geschäftsgeheimnisse im Sinne des § 2 Nr. 1 GeschGehG („Geschäftsgeheimnisse“) des Arbeitgebers zu schützen und sie nicht zu erlangen, zu nutzen oder offenzulegen, soweit deren Erlangung, Nutzung und Offenlegung nicht*
> *a) nach dem GeschGehG (Geschäftsgeheimnisgesetz) oder*
> b) *der einschlägigen arbeitsgerichtlichen Rechtsprechung unter Berücksichtigung der arbeitsrechtlichen Verschwiegenheits- und Loyalitätspflichten des Arbeitnehmers zulässig ist.*

Sollen arbeitsrechtliche Konsequenzen an Verstöße geknüpft werden können, muss ebenfalls auf Konkretheit und Verständlichkeit der Regelungen geachtet werden. Einem Angestellten muss klar sein, was er darf und was nicht.

[6] Beispiel zur Illustration, ohne Gewähr

[7] Beispiel zur Illustration, ohne Gewähr

6.4.2 Whistleblowing

Ausdrücklich hervorgehoben wurde bereits in der Gesetzesbegründung, dass § 5 Nr. 2 GeschGehG dem Schutz der so genannten Whistleblower dienen soll. Zunächst wurde, konsequenterweise gemäß Rechtfertigungslösung, ergänzend ausgeführt, die Regelung stelle klar, dass neben der Erlangung, die Nutzung und die Offenlegung von Informationen über rechtswidrige Handlungen und ein berufliches oder sonstiges Fehlverhalten unter den genannten Voraussetzungen gerechtfertigt sei. [8]

Praxistipp

Der Begriff „Whistleblowing“ kommt aus den USA und bedeutet soviel wie „Verpfeifen“. Whistleblower sind damit „Verpfeifer“ oder auch Hinweisgeber.

Es ist zu klären, ob und wenn ja, unter welchen Voraussetzungen Beschäftigte, die Kenntnis von solchen Informationen über rechtswidrige Handlungen oder sonstige Fehlverhaltensweisen haben, sich unmittelbar an Dritte, beispielsweise Aufsichtsbehörden oder gar die Staatsanwaltschaft, wenden dürfen.

Am 23. Oktober 2019 trat die Richtlinie (EU) 2019/1973 des Europäischen Parlaments und des Rates zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden in Kraft.

7 Durchsetzung von Ansprüchen

§§ 6 ff. GeschGehG enthalten spezielle zivilrechtliche Ansprüche für den Fall einer Geschäftsgeheimnisverletzung. Als Anspruchsgegen kommt der Inhaber des Geschäftsgeheimnisses (§ 2 Nr. 2 GeschGehG) in Betracht. Anspruchsgegen ist der Rechtsverletzer i.S.d. § 2 Abs. 1 Nr. 3 GeschGehG. Ist der Rechtsverletzer ein Beschäftigter eines Unternehmens, so kann der Inhaber dieses Unternehmens als weiterer Anspruchsschuldner hinzutreten (vgl. § 12 GeschGehG).

Sofern der Rechtsverletzer die Rechtsverletzung aus grober Fahrlässigkeit oder mit Vorsatz, also schuldhaft, begangen hat, steht dem Inhaber des Geschäftsgeheimnisses ein Anspruch auf Schadensersatz des aus der Rechtsverletzung (konkret) entstandenen Schadens zu (§ 10 GeschGehG). Bei der Bemessung des Schadens kann z. B. der Gewinn berücksichtigt werden, den der Rechtsverletzer erzielt hat.

Grundsätzlich kann auch Schadensersatz für immateriellen Schaden verlangt werden.

Verjährungsansprüche ergeben sich u.a. nach § 61 Abs. 2 HGB.

[8] BT-Drs. 19/4724, S. 29

8 Datenschutzrechtliche Rahmenbedingungen der Schutzmaßnahmen

Der Zweck heiligt nicht die Mittel. Konkret bedeutet das, dass nicht alles, was zum (technisch-organisatorischen) Schutz von Geschäftsgeheimnissen getan werden kann, auch getan werden darf. Die Maßnahmen zum Schutz von Geschäftsgeheimnissen müssen auch am Datenschutzrecht austariert sein.

Das GeschGehG ist für sich keine Rechtsgrundlage zur Verarbeitung personenbezogener Daten und gibt vor allem nicht die Art und das Ausmaß vor. Hier kommen die datenschutzrechtlichen Grenzen hinzu.

Hieran ändert auch nichts, wenn diese Maßnahme (auch) mit der Sicherheit der Verarbeitung nach Art. 32 DS-GVO begründet werden kann. Denn für die Maßnahmen nach Art. 32 DS-GVO ist ebenso anerkannt, dass sie ihre Grenzen in den übrigen Regelungen des Datenschutzrechts finden.

Diese Elemente sollten bereits bei der Planung der Maßnahmen im Schwerpunkt im Auge behalten werden: Festlegung der Rechtsgrundlage, da sich hieraus Vorgaben für die weiteren Elemente ergeben können; Begrenzung der Verarbeitung auf die begründbar erforderlichen Daten, Transparenz gegenüber den betroffenen Personen.

Keine Angst vor der Pflicht zur Transparenz. Es müssen nicht alle Details offengelegt werden, aber zu bedenken ist, dass das Wissen um Schutzmaßnahmen auch abschreckend wirken kann.

9 Fazit

Das Ziel eines Compliance-Management-Systems (CMS) sollte dabei nicht aus den Augen verloren gehen: Ziel eines wirksamen CMS ist der **Schutz von Mitarbeitern, Führungskräften und Stakeholdern.**

Für ein erfolgreiches Compliance-System ist die Unternehmensleitung daher sehr wichtig. Maßgeblich sind außerdem die Vorbildfunktion von Fach- und Führungskräften sowie den Leitungsorganen, die Kommunikation von Werten und das kompromisslose Sanktionieren von „Non-Compliance“.

Nicht-befolgen („Non-Compliance“) hat Konsequenzen. Für den Einzelnen, z.B. Abmahnung und Entlassung, aber auch für die ganze Organisation, z.B. Sanktionen, Bußgeld, Reputationsverlust.

Compliance ist eine zentrale Voraussetzung für langfristigen und nachhaltigen unternehmerischen Erfolg. Verlässlichkeit, Kontinuität und Vertrauen können in einem Unternehmen nur bestehen, wenn sich dieses deutlich, auch nach außen, zu Compliance bekennt.

Praxistipp

Was sind Stakeholder?

Stakeholder sind alle internen und externen Personengruppen, die von den unternehmerischen Tätigkeiten direkt oder indirekt betroffen sind (Anspruchsgruppen). Eine erfolgreiche Unternehmensführung muss die Interessen und Erwartungen aller Anspruchsgruppen bei den Entscheidungen berücksichtigen. Es sind dabei zwei Stakeholder-Gruppen zu unterscheiden:[9]

- Stakeholder im weiteren Sinne: Demnach sind Stakeholder im weiteren Sinne alle jene, die ein Unternehmen beeinflussen oder von einem Unternehmen beeinflusst werden. Zu ihnen gehören Interessengruppen, Protestbewegungen oder Gewerkschaften.
- Stakeholder im engeren Sinne: Stakeholder im engeren Sinne sind solche, von denen ein Unternehmen *systematisch* abhängig ist. Zu ihnen gehören (potentielle) Mitarbeiter, Zulieferer, Kunden, aber auch die Shareholder und andere mehr.

10 Links

- Gesetz zum Schutz von Geschäftsgeheimissen vom 18. April 2018 (BGBl. I S. 466)

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

- Geschäftsgeheimnisgesetz verabschiedet – Was bedeutet das für Unternehmen, was ist zu tun?

  https://www.adorgasolutions.de/geschaeftsgeheimnisgesetz-geschgehg-verabschiedet/

- Compliance ist mehr als nur Gesetze einhalten

  https://www.die-fuehrungskraefte.de/aktuell/perspektiven-fachzeitschrift/inhaltsverzeichnis-09-102019/compliance-ist-mehr-als-nur-gesetze-einhalten/

11 Abbildungsverzeichnis

[9] Lies, J., (2012), Publik Relations als Machtmanagement, Springer Gabler, Wiesbaden.

12 Autoren

Regina Mühlich ist Geschäftsführerin der Managementberatung AdOrga Solutions GmbH. Sie ist Expertin für Datenschutz, Sachverständige für EDV und Datenschutz (TÜV) sowie Datenschutz-Auditorin (TÜV, DEKRA), Qualitätsmanagementbeauftragte (DQS) und Compliance Officer (Beck-Akademie). Als. Datenschutzbeauftragte berät und unterstützt sie nationale und internationale Unternehmen aus unterschiedlichsten Branchen. Im Datenschutz ist sie seit über 20 Jahren tätig. Sie ist gefragte Referentin für Seminare und Vorträge sowie Mitglied des Vorstandes des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Dr. Jens Eckhardt ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Datenschutz-Auditor (TÜV) und Compliance Officer (TÜV). Seit 2001 ist er in den Bereichen Datenschutz, Marketing, Informationstechnologie und Telekommunikation sowohl strategisch beratend als auch gerichtlich bundesweit tätig. Außerdem ist er Dozent zum Datenschutzrecht an der Ulmer Akademie für Datenschutz und IT-Sicherheit (udis) gGmbH sowie Mitglied des Vorstandes des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Für weitere Informationen

Regina Mühlich
AdOrga Solutions GmbH

E-Mail: rm@AdOrgaSolutions.de
www.AdOrgaSolutions.de

Dr. Jens Eckhardt
Derra, Meyer & Partner Rechtsanwälte PartG mbB
E-Mail: eckhardt@derra-de.de
www.derra.eu

* Hinweis: Der Übersichtlichkeit wegen werden im Folgenden nur die männlichen Formen verwendet.