

1.4. Know-how und Geschäftsgeheimnisse im Kontext internationaler Wirtschaftsbeziehungen

Geschäftsgeheimnisse halten sich nicht an Grenzkontrollen, weder innerhalb der EU noch im interkontinentalen Wirtschaftsverkehr. Die Bedrohungen durch (Betriebs-)Spionage im **Cyberspace** und die immer weiter fortschreitende technische Entwicklung der dabei eingesetzten Mittel werden größer. Dabei erlauben die angewandten Methoden den Diebstahl und Transfer von großen Datenmengen, ohne dass die Täter ihren Schreibtisch bzw meist ihren Computerarbeitsplatz verlassen. Dieses Bedrohungspotenzial haben nicht nur die USA, sondern auch die EU erkannt. Die USA sprechen auch klar aus, dass sie die Regierungen von China und Russland als besonders aggressiv und gefährlich einstufen, was die widerrechtliche Aneignung von Geschäftsgeheimnissen und die dadurch verursachten wirtschaftlichen Schäden sowohl für die einzelnen Unternehmen als auch die Wirtschaft insgesamt anbelangt.⁸

1.4.1. Unterschiedliche Schutzniveaus

Die in den Mitgliedstaaten der EU sehr verschieden gestalteten rechtlichen Regelungen waren Beweggründe für die Vereinheitlichung der Definition von Geschäftsgeheimnissen und geschütztem Know-how. Diese Unterschiede können eine Erleichterung für die Einfuhr von Produkten aus Drittländern in die EU über Einfuhrstellen mit geringem Schutzniveau darstellen in Fällen, in denen Konzeption, Herstellung oder Vermarktung der Produkte auf gestohlenen oder anderen unrechtmäßig erworbenen Geschäftsgeheimnissen beruhen. Auch die Schaffung von kohärenten Schutzmöglichkeiten bei der Rechtsdurchsetzung vor den Gerichten ist daher essenziell. So erwähnt dies die Richtlinie des Europäischen Parlaments und des Rates in den Erwägungsgründen zur RL-Geschäftsgeheimnisse, die der Novellierung des UWG 2018 zugrunde lag.⁹

Durch diese Vereinheitlichung beim Schutz der Geschäftsgeheimnisse und bei der gerichtlichen Durchsetzung im Fall von Verletzungen sollte auch die Bedeutung des Europäischen Wirtschaftsraums als einheitlich geschützte Region steigen und die Tatsache, dass sie aus vielen, im internationalen Vergleich kleinen Nationalstaaten besteht, keinen Nachteil mehr darstellen. Dieses Asset soll europäischen und österreichischen Unternehmen – etwa bei Investitionsentscheidungen im Bereich der Forschung und Entwicklung (F&E) – durchaus bewusst sein.

1.4.2. Internationale Abkommen

Sobald ein Unternehmen in Handelsbeziehungen mit Geschäftspartnern aus dem Ausland tritt, stellen sich Fragen nach den anwendbaren rechtlichen Regelungen.

8 Yeh, Protection of Trade Secrets: Overview of Current Law and Legislation, 15, <https://fas.org/sgp/crs/secretcy/R43714.pdf> (24.3.2020).

9 ErwGr 9 RL-Geschäftsgeheimnisse.

5. Compliance und Haftung

5.1. Compliance – Mission possible?

Der Begriff „Compliance“ hat längst Eingang in das tägliche Wirtschaftsleben gefunden, sogar der Duden kennt ihn und definiert ihn als „regelgerechtes, vorschriftsgemäßes, ethisch korrektes Verhalten“.⁵² Damit ist gleichzeitig ein Auftrag an eine Unternehmensführung verbunden, sich all dieser Pflichten bewusst zu sein und dementsprechend zu agieren und vorzuzorgen.⁵³

Die Anforderungen an ein Compliance Management sind hoch; so umfangreiche und unterschiedliche Materien wie

- das Arbeitsrecht, etwa die Einhaltung von Bestimmungen zur Arbeitszeit, zur Gleichbehandlung, zur Einbindung von Betriebsräten;
- das Kapitalmarktrecht mit Bestimmungen über den Erwerb eigener Aktien, oder der Insiderhandel;
- Steuerrecht;
- IT-Sicherheit, Schutz von Cyber-Angriffen, Vermeidung von Geschäften mit Scheinfirmen;
- personenbezogener Datenschutz;
- das Kartellrecht, zur Vermeidung von unzulässigen Absprachen mit Mitbewerbern;
- die Regeln zur Produktsicherheit und -haftung;
- die Verhinderung von Wirtschaftskriminalität wie Bestechung, Geldwäsche und Betrug

müssen beachtet und erfasst werden.

An der Schnittstelle von Compliance und Geschäftsgeheimnis ergibt sich damit eine Vielzahl an Aufgaben, die von einem Unternehmen bzw dessen Geschäftsführung⁵⁴ zu erbringen sind. Diese sollen im nachfolgenden Kapitel dargestellt werden.

5.1.1. Aufbau von Compliance-Maßnahmen

Nicht jedes Unternehmen ist gleich strukturiert. In einigen Branchen überwiegen technische Aspekte, wie die Entwicklungsabteilung, in manchen fehlt eine solche

52 <https://www.duden.de/rechtschreibung/Compliance> (24.3.2020).

53 *Felll/Pucher*, Corporate Compliance im österreichische Recht – Ein Überblick, wbl, 2010, 265.

54 *Aigner/Aigner/Aigner*, Corporate Governance (Teil II), CFOaktuell 2017, 148.

Was ist Voraussetzung für den Schutz von Geschäftsgeheimnissen nach dem UWG 2018?

Geeignete, den Umständen angemessene Geheimhaltungsmaßnahmen:

- Dienstvertragliche Regelungen,
- Interne Richtlinien/Schulung von Mitarbeitern,
- Vereinbarungen mit Dienstnehmern, die Unternehmen verlassen („exiting employees“),
- physische Zugangskontrollen/Vergabe von kontrollierten Zugriffsrechten in der IT/Clean-Desk-Policy („need-to-know“ Prinzip),
- Interne Organisationsstruktur/Berichtswesen.

5.2. Haftung für das Bestehen von Compliance-Maßnahmen

5.2.1. Delegieren an die zuständige Abteilung?

Wer aber ist nun zuständig für die Einrichtung und Umsetzung dieser Maßnahmen zum Schutz von Geschäftsgeheimnissen? Kann das nicht die Compliance-Abteilung sein, so es eine gibt? Kann das nicht die Personalabteilung – HR sein, die es in der einen oder anderen Form in jedem Unternehmen gibt? Nein, jedenfalls nicht alleine.

5.2.2. Aufgabe der Geschäftsführung

In kleinen Unternehmen, die in Form von Einzelunternehmen strukturiert sind, liegt die Verantwortung für den Schutz von Geschäftsgeheimnissen beim Unternehmer selbst. Die RL-Geschäftsgeheimnisse bezeichnet kleine und mittlere Unternehmen (KMU) als solche, die Geschäftsgeheimnisse in besonderem Maße schätzen und stärker auf sie angewiesen sind.⁵⁸ Sie sollten daher deren Schutz keinesfalls auf die leichte Schulter nehmen.

Unabhängig von der Größe ist die häufigste rechtliche Struktur für ein Unternehmen in Österreich die GmbH. Nach dem GmbHG liegt die Verantwortung für das Handeln der Gesellschaft bei ihren Organen, den Geschäftsführern. Diese haben nach § 25 GmbHG bei ihrer Geschäftsführung die **Sorgfalt eines ordentlichen Geschäftsmannes** anzuwenden, dazu sind sie der Gesellschaft gegenüber verpflichtet. Eine Verletzung dieser Pflicht zieht auch eine Haftung der Geschäftsführer nach sich. Sie sind somit im Interesse der Gesellschaft wie auch in ihrem eigenen Interesse dazu angehalten, sich über das Thema des Schutzes der Geschäftsgeheimnisse Gedanken zu machen und sich damit ausreichend auseinanderzusetzen.

58 ErwGr 2 RL-Geschäftsgeheimnisse.

Praxisbeispiel

Ein Produktionsbetrieb stellt regelmäßig und saisonbedingt massiven Schwund der hergestellten Produkte fest. Eine externe Whistleblowing-Hotline soll eingerichtet werden, bei der Mitarbeiter ihre Beobachtungen melden können. Da es sich aber hier nicht um Vergehen der Korruption, Bestechung, Verstöße gegen Buchführungsvorschriften und Steuerhinterziehung, illegale Praktiken, wie Geldwäsche und Bankenbetrug, oder Fälschung von Finanzunterlagen und Insiderhandel handelt, sondern allenfalls um Diebstahl, ist hier eine Whistleblowing-Hotline datenschutz- und arbeitsrechtlich nicht zulässig. Es müssen andere geeignete, interne Maßnahmen getroffen werden, um das zulässige Interesse des Unternehmens an der Aufklärung und Verhinderung zukünftiger Vorfälle zu wahren. Im Ergebnis lässt sich also nicht jeder Sachverhalt mit einer Whistleblowing-Hotline regeln.

6.3. EU Whistleblower-Richtlinie

Auch die EU hat in diesem Zusammenhang Handlungsbedarf erkannt und daher eine eigene Richtlinie zu Meldung von Verstößen gegen Unionsrecht beschlossen (Whistleblower-RL).⁶⁵ Durch die uneinheitliche Situation dieses Rechtsbereichs in den einzelnen Mitgliedstaaten hinkt die EU hier den USA hinterher. Die Richtlinie ist bis Mai 2021 in nationales Recht aller EU-Mitgliedstaaten umzusetzen, sollte aber jedenfalls schon vorher beachtet werden.

Der Kreis möglicher Meldungen ist beschränkt, betrifft aber im Gegensatz zur Regelung in den USA (Sarbanes-Oxley Act 2002) keineswegs nur Wirtschaftsdelikte. Die Aufzählung von Verstößen, die unter die Anwendung dieser Richtlinie fallen, ist lang.⁶⁶ Sie umfasst unter anderem neben den klassischen Materien **Finanzvergehen, Betrugsbekämpfung und öffentliches Auftragswesen** auch Bereiche wie **Produkt- und Lebensmittelsicherheit, Umwelt- und Verbraucherschutz** sowie Datenschutz und die Sicherheit von Netz- und Informationssystemen. Ausdrücklich ausgenommene Bereiche sind jedenfalls das EU-Arbeitsrecht – nicht, weil es nicht als schutzwürdig angesehen wird, sondern weil hier bereits andere Rahmenrichtlinien bestehen – sowie die nationale Sicherheit.

Gerade durch die Möglichkeit, Verstöße gegen das Unionsrecht in Bereichen wie Produkt- und Lebensmittelsicherheit, Umwelt- und Verbraucherschutz zu melden, besteht die Möglichkeit, dass dadurch Geschäftsgeheimnisse offengelegt werden. Die Whistleblower-RL trägt diesem Spannungsverhältnis Rechnung. Wer im beruflichen Kontext Informationen erlangt, aufgrund derer er Beweise für tatsächliche Verstöße oder begründete Verdachtsmomente dahingehend hat, dass ein Verstoß gegen EU-Recht vorliegt, hat als Hinweisgeber Anspruch auf Schutz

65 RL (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

66 RL (EU) 2019/1937, Art 2, Abs (1) a) i) bis x), b), c).

7.2.5. Betriebsvereinbarungen

Wenn im Unternehmen ein **Betriebsrat** besteht, können Regelungen mit **Gültigkeit für alle** Arbeitnehmer über zwischen Arbeitgeber und Betriebsrat abgeschlossene Betriebsvereinbarungen festgeschrieben werden, die ansonsten mit allen Mitarbeitern einzelvertraglich über die Verpflichtung zur Einhaltung von Geheimnisschutz-Richtlinien vereinbart werden müssen. Dabei müssen sogenannte normative Betriebsvereinbarungen ausdrücklich im Gesetz (wie etwa im Arbeitsverfassungsgesetz, Arbeitszeitgesetz und Urlaubsgesetz) vorgesehen oder durch eine Ermächtigung in einem Kollektivvertrag gedeckt sein. Bei diesen normativen Betriebsvereinbarungen werden je nach Regelungsinhalt die vier nachstehend dargelegten Arten unterschieden.

Notwendige Betriebsvereinbarungen ohne die Möglichkeit der Anrufung einer Schlichtungsstelle regeln sensible Materien, wie die Einführung einer betrieblichen Disziplinarordnung, über allgemeine Angaben zur Person und Qualifikation hinausgehende Personalfragebögen und **Kontrollmaßnahmen, die die Menschenwürde berühren**.⁸³ Die in Kapitel 7.2.6. genannten Software-Programme zur Kontrolle von Datenflüssen und Zugriffen könnten in die letzte Kategorie fallen und eine solche Betriebsvereinbarung für ihre Rechtswirksamkeit erfordern.

Notwendige Betriebsvereinbarungen mit der Möglichkeit der Anrufung der Schlichtungsstelle sind für die Einführung von Systemen der automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von **personenbezogenen Daten der Arbeitnehmer**, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen, soweit die Verwendung der gewonnenen Daten über die Erfüllung gesetzlicher und (kollektiv-)vertraglicher Verpflichtungen hinausgeht, sowie für die Einführung von Systemen zur Beurteilung von Arbeitnehmern mit Datenerhebungen, die nicht durch die betriebliche Verwendung gerechtfertigt sind, vorgesehen.⁸⁴ Hier lässt sich die Verwendung von personenbezogenen Daten, die sich aus den genannten Kontrollmaßnahmen ergeben, mit der Erfüllung der gesetzlichen Verpflichtungen zum Geheimnisschutz und der Schadensminderung argumentieren.

Durch die Schlichtungsstelle erzwingbare Betriebsvereinbarungen umfassen Bereiche wie allgemeine **Ordnungsvorschriften**, Maßnahmen zur zweckentsprechenden **Benützung von Betriebseinrichtungen und Betriebsmitteln** etc.⁸⁵ Hierunter können zB räumliche und technische Maßnahmen zum Schutz von Geschäftsgeheimnissen fallen. Schließlich können über fakultative Betriebsvereinbarungen Maßnahmen zur Sicherung der von Arbeitnehmern eingebrachten Gegenständen, betriebliches Beschwerdewesen etc geregelt werden.⁸⁶

83 § 96 ArbVG.

84 § 96a ArbVG.

85 § 97 Abs 1 Z 1–6a ArbVG.

86 § 97 Abs 1 Z 7–26 ArbVG.

Was ist bei Kooperationspartnern besonders zu beachten und vertraglich abzusichern?

- Background Check vor Vertragsabschluss,
- Vertraulichkeitsvereinbarung (NDA) und Vorvereinbarung (LOI) vor Beginn der Vertragsverhandlungen,
- Bestandsaufnahme für die geplanten Inhalte der Kooperation,
- Regelungen zu Verwertungsbeschränkungen und Exklusivität,
- unbefristete Geheimhaltungsverpflichtung auf Basis der konkret betroffenen Geschäftsgeheimnisse mit Vertragsstrafe bei Verletzung – keine Standardklauseln,
- Verpflichtung nachweisbarer angemessener Geheimhaltungsmaßnahmen durch alle Kooperationspartner,
- Ausschluss oder Einschränkung von „Reverse Engineering“ durch die Kooperationspartner,
- Vertragsklausel zu anwendbarem Recht und Gerichtsstand bzw Mediations- und Schiedsklausel.

7.5. Externe Dienstleister und Berater

7.5.1. Besonders geheimnis-relevante Bereiche

Externe Dienstleister und Berater bergen vor allem dort ein Gefahrenpotenzial, wo keine berufs- und **standesrechtlichen Verschwiegenheitspflichten**, wie bei Ärzten, Steuerberatern und Wirtschaftsprüfern sowie Rechtsanwälten, bestehen. Abgesehen vom Outsourcing unterschiedlichster Unternehmensdienstleistungen sind vor allem die Bereiche **PR-Beratung und Marketing, Personalberatung, Wirtschaftscoaching, IT, Reinigung und Entsorgung** besonders sensible und oft mangels entsprechendem Bewusstsein nicht ausreichend geschützte Bereiche. Industriespionage wird in der Praxis nicht nur über untreue (IT-)Mitarbeiter oder externe Hacker abgewickelt, sondern nicht selten über eingeschleustes „Reinigungspersonal“, das sich mit umfassenden Zutrittsberechtigungen außerhalb der Bürozeiten an Geschäftsgeheimnissen „bedient“.

Auch hier ist daher schon vor dem Eingehen der Geschäftsbeziehung ein sorgfältiger **Background Check** des künftigen Vertragspartners zu empfehlen, um dessen Vertrauenswürdigkeit, Verlässlichkeit und bisheriges Verhalten am Markt abzuklären. Zusätzlich ist es bereits in der Phase der Vertragsverhandlungen zweckmäßig, vor der Weitergabe von Informationen, die Geschäftsgeheimnisse enthalten, an den künftigen Geschäftspartner zu diesen eine **Vertraulichkeitsvereinbarung** abzuschließen.

Die Vereinbarung einer exklusiven Zusammenarbeit ist hier kaum möglich, da gerade externe Dienstleister und Berater mit ihrer **Branchenkenntnis** am Markt punkten. Die Tatsache, dass nicht alle Besonderheiten einer Branche erklärt werden müssen, weil dazu ein Vorwissen aus anderen Geschäftsbeziehungen besteht, hat grundsätzlich Vorteile. Allerdings birgt dies auch das gewisse Risiko, dass

8. Wertvolles Know-how und die kartellrechtlichen Schranken der Verwertung

8.1. Warum Kartellrecht?

Sowohl das österreichische Kartellgesetz als auch das EU-Kartellrecht haben eine gemeinsame Zielsetzung: ein hohes Maß an Wettbewerb zwischen den Unternehmen zu fördern. Die damit verbundenen positiven Auswirkungen auf die Verbraucher sollen sich in niedrigen Preisen, vielfältigem Angebot und der Entwicklung immer neuerer und besserer Produkte äußern. Daher sind alle **Vereinbarungen, Absprachen und abgestimmten Verhaltensweisen** zwischen Unternehmen, welche den Handel zu beeinträchtigen geeignet sind und eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken, verboten.⁸⁸ Die Frage, ob auf einen Fall nationales oder EU-Kartellrecht anwendbar ist, richtet sich danach, ob eine Beeinträchtigung des Handels zwischen den Mitgliedstaaten oder nur innerhalb eines EU-Mitgliedstaats im Raum steht. Wesentliche inhaltliche Unterschiede in Bezug auf die Beurteilung, ob eine Wettbewerbsbeschränkung vorliegt, bestehen dabei nicht.

Die Entwicklung von Know-how, von neuen Technologien und besseren Produkten ist aber nicht immer und in allen Fällen nur durch einzelne Unternehmen sinnvoll. Die Zusammenführung von Forschungsergebnissen und die gemeinsame Entwicklung von Produkten sowie deren nachfolgende Vermarktung oder Lizenzierung erfolgen im Wirtschaftsleben oft durch die Zusammenarbeit von zwei oder mehreren Partnern, zum besseren Nutzen und Erfolg der Beteiligten.

Unternehmen sind dabei gut beraten, ihre Zusammenarbeit vorab schriftlich zu regeln. In Verträgen über **Forschungs- oder Entwicklungszusammenarbeit (F&E-Verträge)** finden sich meist auch Berührungspunkte mit dem Kartellrecht, da in solchen Vereinbarungen potenziell Regelungen getroffen werden, die geeignet sind, den Wettbewerb zu beschränken. Gerade Forschungs- und Entwicklungszusammenarbeit, aber auch **Technologietransfer** beeinflussen den Innovationswettbewerb und auch den wirtschaftlichen und technischen Fortschritt. Schon eine Geheimhaltungsvereinbarung ist hier an sich nicht wettbewerbsfördernd, weil wertvolles Wissen vom Markt ferngehalten wird. Aber auch Vereinbarungen, wonach Vertragspartner sich darauf verständigen, keinen weiteren Forschungs- und Entwicklungstätigkeiten im selben Feld nachzugehen, können sich wettbewerbs-

⁸⁸ Art 101 AEUV; § 1 Kartellgesetz 2005 (BGBl I 2005/61) idgF.

10.3. Strafbarkeit von Verletzungen des UWG

Auch das UWG selbst enthält Bestimmungen über gerichtlich strafbare Handlungen, die nur auf Verlangen des Verletzten, also als **Privatanklageverfahren**, zu verfolgen sind. Es sind dies die Bestechung von Bediensteten oder Beauftragten nach § 10 UWG, die Verletzung von Geschäfts- oder Betriebsgeheimnissen nach § 11 UWG sowie der Missbrauch anvertrauter Vorlagen nach § 12 UWG.

Die praktische Bedeutung dieser Bestimmungen ist in Bezug auf die sog. „Privatkorruption“ nach § 10 UWG sehr beschränkt. Nach einer Entscheidung aus den 1970er Jahren beschäftigten sich die Gerichte erst wieder im Jahr 2018 mit einem Fall, der als Ergebnis ua klarstellte, dass Geschenke, die als „sozialadäquate Zuwendungen“ anzusehen sind, den Tatbestand der Bestechung nicht erfüllen.¹¹⁴ Von § 10 UWG soll der lautere Wettbewerb vor der Begünstigung und Bevorzugung vor anderen Mitbewerbern geschützt werden, die nicht mittels Geschenken oder anderer Vorteilen „schmieren“, um ihre Waren oder Dienstleistungen abzusetzen.

Die strafbare Verletzung von Geschäfts- oder Betriebsgeheimnissen ist hingegen regelmäßig Gegenstand von Gerichtsverfahren. Je erfolgreicher die praktische Umsetzung der neuen zivilrechtlichen Bestimmungen über den Schutz von Geschäftsgeheimnissen gelingt, desto eher kann man erwarten, dass die Strafverfahren an Bedeutung verlieren. Primäres Interesse von Unternehmen ist wohl, den Schutz ihres wertvollen Know-how durch Unterlassungsansprüche, Entgelt- und Schadenersatzzahlungen zu schützen, statt Strafverfahren mit den bereits dargestellten Risiken zu führen.

Die strafbare Verletzung von Geschäfts- oder Betriebsgeheimnissen hat dabei in der Praxis unter anderem auch in Bezug auf **Vergabeverfahren**, die ja häufig und aus unterschiedlichen Aspekten rechtlich bekämpft werden, Bedeutung. Ein Informationsvorteil im Vergabeverfahren kann durchaus die Marktsituation eines Mitbewerbers beeinflussen. Wie der OGH klargestellt hat, genügt es für eine Strafbarkeit von Bediensteten, die ein ihnen anvertrautes Geschäftsgeheimnis während des Dienstverhältnisses unbefugt an andere weitergeben, wenn dadurch die Wettbewerbssituation eines oder mehrerer Mitbieter im Vergabeverfahren gefördert wird. Das UWG schützt nach der sog. „Schutzzwecktrias“ des OGH nicht mehr nur ausschließlich die Interessen der Mitbewerber an einem lauterem Wettbewerb, sondern erfasst auch die Interessen der Allgemeinheit und Verbraucher.¹¹⁵

Dabei ist auf eine wesentliche Unterscheidung zwischen der Verletzung von Geschäfts- und Betriebsgeheimnissen nach § 11 UWG und nach den zivilrechtlichen Bestimmungen hinzuweisen: strafbar ist ein Dienstnehmer, der das Geschäfts-

114 OGH 29.1.2018, 4 Ob 252/18i.

115 OGH 28.8.2012, 12 Os 38/12y.

11. Zivilrechtliche Maßnahme

11.1. Das neue Geheimnisschutz-Verfahren nach UWG

Mit der Novelle 2018 zum UWG wurde ein ganzes Set an Maßnahmen zum Schutz von Geschäftsgeheimnissen zur Durchsetzung von Ansprüchen auf **Unterlassung**, **Beseitigung** von rechtsverletzenden Produkten, **Schadenersatz** und **Herausgabe des Gewinns** eingeführt.

Diese schaffen nicht nur erstmals eine gesetzliche Definition, was als Geschäftsgeheimnis zu verstehen ist, sondern auch Sonderbestimmungen darüber, wie in einem **Gerichtsverfahren** die Vertraulichkeit von Geschäftsgeheimnissen gewahrt werden kann. Damit soll vermieden werden, dass im Rahmen der Beweispflicht erst recht Geschäftsgeheimnisse offengelegt werden müssen, obwohl sie eigentlich genau davor geschützt werden sollen. Damit soll der von der zugrunde liegenden Idee der Stärkung des Schutzes von Geschäftsgeheimnissen getragenen Intention der RL-Geschäftsgeheimnisse, die mit dieser Novelle umgesetzt wurde, Rechnung getragen werden.

11.2. Drei Schritte zum Erfolg

Was ist nun zu unternehmen, wenn der Verdacht besteht, dass ein Geschäftsgeheimnis bedroht ist, verletzt zu werden, oder die Verletzung bereits erfolgt ist und unterbunden werden soll? Macht es Sinn, den Gerichtsweg zu beschreiten? In den meisten Fällen wohl ja. Denn wer nicht kämpft, hat schon verloren.

Kurz zusammengefasst sind in einem Gerichtsverfahren folgende drei Schritte zu setzen.

- 1) Sicherungsverfahren – zur Sicherung von Beweismitteln und für einstweilige Maßnahmen.
- 2) Hauptverfahren – zur Entscheidung über das Bestehen und die Verletzung des Geschäftsgeheimnisses.
- 3) Durchsetzung – der Ansprüche auf Unterlassung, Beseitigung, Schadenersatz und Herausgabe des Gewinns.

Danach gliedert sich die Vorbereitung, die zwischen Unternehmen, den betreuenden Rechtsanwälten und gegebenenfalls beizuziehenden weiteren Experten detailliert abgestimmt werden muss.

12. Alternatives Streitbeilegungsverfahren

12.1. Auswirkungen von Gerichtsverfahren

Eines darf dabei nicht vergessen werden: zieht man zu vor, sind in der Praxis meist schon einige Versuche zur Beilegung der Auseinandersetzung oder Vermeidung eines Verfahrens gescheitert. Man hat den Mitbewerber bereits angesprochen, eventuell schriftlich abgemahnt oder sich auf Managementebene getroffen, ohne eine gütliche Einigung zu finden. In Fällen, in denen ein direkter Mitbewerber geklagt wird, sind solche Überlegungen, wie die durch ein Gerichtsverfahren endgültig zerstörte Gesprächsbasis, kaum von Belang. Eher relevant kann die Tatsache sein, dass trotz aller oben dargestellten Maßnahmen zur Wahrung der Vertraulichkeit von Geschäftsgeheimnissen jedenfalls der Umstand, dass ein Gerichtsverfahren anhängig ist, in der Branche bekannt wird. Im Fall der Entscheidung durch Urteil, insbesondere durch eine Berufungsinstanz oder letztlich den OGH, kann auch die Veröffentlichung der Entscheidung, trotz Anonymisierung und nicht vertraulicher Urteilsfassung, für Gesprächsstoff sorgen.

Besteht allerdings in einer Kunden-Lieferantenbeziehung oder zwischen – ehemaligen oder bestehenden – Partnern in einer Forschungs- und Entwicklungskooperation ein Konflikt, liegt oftmals eine Zusammenarbeit der Parteien auch in Zukunft in beiderseitigem Interesse. Diese zukünftige Beziehung zu erhalten, wird durch ein Gerichtsverfahren wohl zumindest erschwert oder gar unmöglich gemacht. Vor Gericht gibt es Verlierer und Gewinner bzw allenfalls Parteien, die sich, eher aus pragmatischen Gründen, vergleichen, sodass sich am Ende oft beide Seiten als Verlierer fühlen.

12.2. Alternative Streitbeilegung

Dazu kommt, dass zwar nach der österreichischen Zivilprozessordnung die Parteien Herr des Verfahrens sind, diese sich aber in der Praxis kaum so fühlen. Das liegt sowohl am Setting eines Gerichtsverfahrens, an der Entscheidung durch das Gericht als einen außenstehenden Dritten und nicht zuletzt an dem Umstand, dass juristische Texte, wie die einzubringenden Schriftsätze und Gerichtsentscheidungen, weder selbsterklärend sind noch die Lieblingslektüre von Managern darstellen. Damit einher geht das Gefühl, die Kontrolle über den weiteren Verlauf des Verfahrens aus der Hand zu geben und nicht mehr selbst steuern zu können, wie sich das Verfahren entwickelt. In der Praxis haben sich daher sogenannte Alternative Streitbeilegungsverfahren oder Alternative Dispute Resolutions (ADR) entwickelt. Dazu