ZIIR - Zeitschrift für Informationsrecht

Was sind angemessene Geheimhaltungsmaßnahmen zum Schutz eines Geschäftsgeheimnisses?

Aufsätze · RA Dr. Georg Bruckmüller · ZIIR 2025, 135 · Heft 2 v. 23.4.2025

Geheimhaltungsklauseln in Arbeitsverträgen allein sind keine angemessenen Geheimhaltungsmaßnahmen. Der OGH fordert zusätzlich ein Maßnahmenkonzept bei Ausscheiden von Mitarbeitern. Welche Maßnahmen Unternehmer zum Schutz von Geschäftsgeheimnissen zu setzen haben, wird die Gerichte noch öfter beschäftigen. Der Beitrag behandelt die erste Entscheidung in Österreich und die Kriterien der deutschen Rechtsprechung dazu.

Deskriptoren: Unlauterbarkeit; Geschäftsgeheimnis; Geheimhaltungsmaßnahmen; Angemessenheit; Verschwiegenheitsverpflichtung; Maßnahmenkonzept.
Normen: § 26b UWG, § 2 GeschGehG

1. Ausgangslage

Die Novelle des UWG[1] hat nicht nur eine Harmonisierung der Bestimmungen zum Schutz von Geschäftsgeheimnissen auf Europäischer Ebene gebracht, sondern auch einen Paradigmenwechsel bei der Erlangung des Know-how-Schutzes und der Durchsetzung des Schutzes eines Geschäftsgeheimnisses bewirkt.

Die gesetzliche Definition des Geschäftsgeheimnisses[2] hat gegenüber der bis 31.1.2019 geltenden Rechtslage im UWG auch eine Einschränkung des Schutzes von Geschäftsgeheimnissen gebracht. Dies zeigt sich darin, dass ein Geschäftsgeheimnis – abgesehen davon, dass dieses nicht allgemein zugänglich sein darf – nur mehr dann vorliegt, wenn a) der Berechtigte zuvor angemessene Geheimhaltungsmaßnahmen gesetzt hat und b) die vertraulichen Informationen einen kommerziellen Wert aufweisen. Wenn eines dieser Tatbestandselemente nicht vorliegt, dann liegt seit der gesetzlichen Änderung kein Geschäftsgeheimnis vor, auch dann, wenn es sich um eine geheime Information handelt und/oder der Unternehmer ein subjektives Geheimhaltungsinteresse an diesen Informationen hat.

Liegen nicht alle drei in § 26b Abs 1 UWG genannten Tatbestandselemente vor, ist nicht nur die Rechtsdurchsetzung gegenüber vermeintlichen Störern verwehrt, sondern ist ein Geschäftsgeheimnis oder ein Recht an einem Geschäftsgeheimnis bei unzureichenden Geheimhaltungsmaßnahmen von vornherein gar nicht entstanden.

Ohne angemessene Geheimhaltungsmaßnahmen des Berechtigten[3] und ohne kommerziellen Wert der Information selbst[4] kann kein rechtswidriger Erwerb, keine rechtswidrige Nutzung und keine rechtswidrige Offenlegung einer vertraulichen betrieblichen oder technischen Information durch Dritte vorliegen. Dem Inhaber von vertraulichen Informationen stehen keine Maßnahmen zum Schutz von Geschäftsgeheimnissen in Gerichtsverfahren[5] und keine Mittel zur Sicherung solcher im Rahmen von Verfahren auf Erlassung einer Einstweiligen Verfügung[6] zu. Diese sich schon aus dem UWG ergebende Erkenntnis hat der OGH nun auch in der Rsp[7] behandelt und lässt sich kurz zusammenfassen: Ohne angemessene Geheimhaltungsmaßnahmen im Unternehmen liegt kein Geschäftsgeheimnis vor.

Herausfordernd für alle Unternehmen ist, dass sie in einem Gerichts- und Provisorialverfahren beweis- und bescheinigungspflichtig für das Vorliegen solcher

angemessener Geheimhaltungsmaßnahmen sind. Oft wird erst durch eine vermeintliche Verletzung von Geschäftsgeheimnissen die Notwendigkeit eines raschen Nachweises, dass Geheimhaltungsmaßnahmen gesetzt wurden, virulent. Für Unternehmer ist es am Naheliegendsten den Nachweis solcher Maßnahmen durch Vorlage von Verschwiegenheitsverpflichtungen, die Arbeitnehmer oder Kooperationspartner im Rahmen der jeweiligen Vertragsbeziehung abgegeben haben, zu erbringen[8].
Für die Unternehmer ist daher die Frage zentral, was alles zu tun ist, damit seine unternehmerischen Informationen dem Geheimnisschutz unterliegen. Was wird verlangt, damit Geschäftsgeheimnisse geschützt sind?

2. Wann liegen angemessene Geheimhaltungsmaßnahmen vor?

Grundsätzlich lassen sich Geheimhaltungsmaßnahmen in rechtliche, technische und organisatorische Maßnahmen unterscheiden. Die Gerichte haben im Einzelfall zu prüfen, ob die getroffenen Geheimhaltungsmaßnahmen ausreichend waren. Dabei besteht ein erheblicher Ermessensspielraum für die Gerichte, die auch auf die jeweiligen Umstände abzustellen haben.[9] So sollen die Größe des Unternehmens, unter welchen Umständen die fraglichen Informationen übermittelt bzw in Erfahrung gebracht werden, die Art und Relevanz der Information und die Erkennbarkeit der Geschäftsgeheimniseigenschaft dafür entscheidend sein, ob ein Geschäftsgeheimnis besteht und rechtlichen Schutz genießt.[10]
Auch wenn betont wird, dass die Anforderungen an angemessene Geheimhaltungsmaßnahmen nicht überspannt werden dürfen, so ist auffällig, dass der Gesetzgeber diese Unschärfen zu Lasten möglicher Geschädigter in Kauf nimmt. Die Know-how-Richtlinie hat nur einen Mindestschutz für Geschäftsgeheimnisse vorgesehen; die Aufrechterhaltung des bisherigen Verständnisses, was ein Geschäftsgeheimnis ist, wäre daher möglich gewesen. Selbst wenn ein subjektives Geheimhaltungsinteresse an einer Information für jedermann evident ist, besteht kein Schutz eines Geschäftsgeheimnisses, wenn der vermeintlich Berechtigte keine Geheimhaltungsmaßnahme nachweisen kann[11].
Dies zeigt auch der Fall, bei dem der OGH[12] sich nun erstmals mit der Frage, was angemessene Geheimhaltungsmaßnahmen sind, beschäftigte. Die Kriterien, die für künftige Fälle maßgeblich sind, sollen im Folgenden näher betrachtet werden.

2.1. Maßnahmenkonzept bei Ausscheiden von Mitarbeitern

Im Rahmen von IT-Sicherheitsmaßnahmen hat der Unternehmer nach der Rsp dafür zu sorgen, dass nicht nur Dritte, sondern auch ehemalige Mitarbeiter keinen Zugang zu vertraulichen Daten haben dürfen. Bei ehemaligen Mitarbeitern fordert der OGH[13] den sofortigen Entzug des Passworts oder die unverzügliche Sperre zum IT-System.
Der OGH[14] wirft dem Antragsteller vor, dass er kein Maßnahmenkonzept betreffend ausscheidende Mitarbeiter behauptet hat. Damit fordert er implizit ein solches Maßnahmenkonzept für Unternehmen. Was darunter zu verstehen ist, musste das Gericht nicht mehr beantworten.
Meines Erachtens ist ein Vorliegen solches unabhängig von der Größe eines Unternehmens. Ein solches Konzept bei Ausscheiden von Mitarbeitern kann durch die Erstellung einer Checkliste, aus der sich Handlungsanweisungen bei der Beendigung von Dienstverhältnissen und Zuständigkeiten für die Umsetzung dieser ergeben, nachgewiesen werden. Maßnahmen können dabei sein, die Überprüfung des Umfanges von Geheimhaltungsvereinbarungen, die Nachholung oder Präzisierung solcher, die sich nur aus der arbeitsrechtlichen Treuepflicht ergeben oder die Erinnerung an Geheimhaltungspflichten. Auf technischer Ebene ist die Abnahme aller Schlüssel und Zutrittskarten, die Sperrung des

Zugangs zu IT-Systemen, e-mail-accounts, eines allfälligen Remote-Zugangs, die Übergabe aller Arbeitsmittel wie Mobiltelefon, Laptop, sonstiger Speichermedien (USB-Sticks und externe Festplatten) und die Änderung von Passwörtern, die dem Mitarbeiter Zugriff zu vertraulichen Daten ermöglichten, in so ein Konzept aufzunehmen.
Ein Maßnahmenkonzept beschränkt sich mE nicht auf Existenz einer solchen Checkliste, sondern es bedarf auch der Festlegung von Verantwortungen für die Einhaltung der Maßnahmen im Unternehmen.
Offen lässt der OGH, ob das Vorliegen eines Maßnahmenkonzepts betreffend ausscheidende Mitarbeiter ausreichend gewesen wäre, wenn aber aufgrund eines Versäumnisses im Unternehmen ausnahmsweise ein ehemaliger Mitarbeiter noch Zugang zu den vertraulichen Daten gehabt hätte. Wenn der Unternehmer darlegen kann, dass der Zugriff zu Geschäftsgeheimnissen auf ein Einzelversagen zurück zu führen ist, dann führt dies mE nicht zum Verlust des Schutzes eines Geschäftsgeheimnisses. Für das Vorliegen eines Geschäftsgeheimnisses ist nicht ein lückenloses Kontrollsystem erforderlich, sondern dass sich Unternehmen um den Schutz der für sie wichtigen Informationen kümmern sollen[15]. Dritten wie Arbeitnehmern und Vertragspartnern des Unternehmens soll klar sein, welche Informationen geheim zu halten sind.

2.2. Zeitlicher Aspekt von Sicherheitslücken
Maßgeblich war für den OGH, dass der Zugang zu den vertraulichen Daten noch Monate nach dem Ausscheiden der Mitarbeiterin nach wie vor möglich war.[16] Zwischen dem Zeitpunkt des Ausscheidens der ehemaligen

Mitarbeiterin Ende Juli 2021 und den Zugriffen auf das IT-System des Unternehmens Mitte November 2021 war genug Zeit den Zugang zu vertraulichen Daten zu unterbinden, so der OGH.
Daraus folgt: Je länger der Zugriff auf vertrauliche Informationen durch ehemalige Arbeitnehmer oder andere Unberechtigte generell möglich ist, desto eher ist davon auszugehen, dass keine angemessenen technischen Sicherheitsmaßnahmen vorlagen.
Allerdings sollte diesem Kriterium mE nicht zu viel Bedeutung beigemessen werden. Es gibt Fälle, in denen der Unternehmer von einer „Sicherheitslücke“ erst durch einen unberechtigten Zugriff erfährt. Je mehr Geheimhaltungsmaßnahmen der berechtigte Unternehmer gesetzt hat, desto weniger maßgeblich ist die Dauer möglicher unberechtigter Zugriffe.

2.3. Anforderungen an Verschwiegenheitsverpflichtungen
Schriftliche Verschwiegenheitsverpflichtungen allein, sei es in Dienstverträgen oder in separaten Erklärungen der Dienstnehmer stellen nach dem OGH keine ausreichende Geheimhaltungsmaßnahme iSd § 26b UWG dar. Unternehmer können sich daher nicht allein auf Verschwiegenheitsverpflichtungen berufen, um einen wirksamen Geheimnisschutz durchzusetzen. Es bedarf weiterer Maßnahmen. Dies gilt auch für alle Know-how betreffende Kooperations- oder Entwicklungsvereinbarungen zwischen Unternehmen.
OGH verwies auf das Rekursgericht[17], das bemängelte, dass sich die Antragstellerin gegenüber der Mitarbeiterin mit einer im Jahr 2018 (also noch zur alten Rechtslage) abgegebenen Verpflichtungserklärung begnügt habe. Das kann als „Fingerzeig“ auf den Inhalt einer solchen Erklärung verstanden werden.
Um sicher zu gehen, sollten daher Unternehmen auf die neue Rechtslage abstellende Verschwiegenheitsverpflichtungen abgeben. Die häufige Praxis, in Arbeitsverträgen – unabhängig von der jeweiligen Position – Mitarbeiter allgemein zur Einhaltung von Betriebs-

und Geschäftsgeheimnissen zu verpflichten, stellt mE keinen angemessenen Schutz von Geschäftsgeheimnissen auf rechtlicher Ebene dar. Arbeitnehmern wird durch derartige „Catch-all“-Klauseln nicht vor Augen geführt, welche Informationen konkret einem Geheimnisschutz unterliegen sollen und welche Handlungen und Unterlassung verboten oder geboten sind.
Hinzu kommt, dass derartige Klauseln uU sogar unwirksam sein können, wenn sie zu einer unzumutbaren Einschränkung der Erwerbsfreiheit führten. Dass diese einem nachvertraglichen Wettbewerbsverbot gleich zu setzen sind und Arbeitnehmer unangemessen benachteiligen, wird für das deutsche Arbeitsrecht, bereits vertreten[18]. Weite Geheimhaltungsklauseln, die einen Arbeitnehmer zur Geheimhaltung sämtlicher betrieblich erlangter Informationen verpflichten, sind demnach unwirksam.[19] In Österreich wird man solche Klauseln allenfalls mit einer geltungserhaltenden Reduktion noch aufrechterhalten können.
Eine (nachvertragliche) Verschwiegenheitsverpflichtung, die dem Erfordernis angemessener Geheimhaltungsmaßnahmen entsprechen soll, muss sich mE auf konkret bestimmbare Geschäftsgeheimnisse beziehen. Dabei ist eine allgemeine Umschreibung, wie etwa Informationen über die Herstellung eines Produktes einschließlich der Rezeptur, aber ausreichend.
Der OGH rügt zwar[20], dass es der Unternehmer unterlassen habe, bei Beendigung des Dienstverhältnisses die ausscheidende Mitarbeiterin an die weitere Einhaltung der Verschwiegenheitsverpflichtung zu erinnern. Daran, dass keine angemessenen, technischen Geheimhaltungsmaßnahmen gesetzt wurden, ändert diese Anmerkung nichts, zeigt aber, dass das Teil eines Maßnahmenkonzepts sein kann. So ist Unternehmen anzuraten, in Kündigungs- und Entlassungsschreiben oder in Vereinbarungen über die Beendigung von Dienstverhältnissen, auf die Einhaltung von Verschwiegenheitsverpflichtungen hinzuweisen. Sinngemäß gilt dies auch für andere Vertragsbeziehungen.

3. Zur deutschen Rechtsprechung

Ein Blick nach Deutschland ist im Bereich der Geschäftsgeschäftsgeheimnisse erlaubt und geboten, da der auf die Know-How-Richtlinie beruhende Gedanke der angemessenen Geheimhaltungsmaßnahmen wie in Österreich übernommen wurde. Die Definition in § 2 Nr 1 GeschGehG fordert – im Unterschied zum Wortlaut des § 26 b UWG – zusätzlich ein berechtigtes Interesse an der Geheimhaltung.

3.1. Kriterien für die Angemessenheit

Bei der Beurteilung der Angemessenheit von Geheimhaltungsmaßnahmen handelt es sich um ein flexibles und offenes Tatbestandsmerkmal, das dem Gedanken der Verhältnismäßigkeit folgt. Die Angemessenheit setzt keinen optimalen Schutz voraus, weil anderenfalls der Geheimnisbegriff zu stark eingeschränkt würde. Es sind

weder die bestmöglichen noch sichersten Maßnahmen erforderlich[21].
Folgende Kriterien sind bei der Beurteilung der Angemessenheit von Bedeutung: Die Art und der wirtschaftliche Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten, die Natur der Informationen, die Bedeutung für das Unternehmen, der Grad des Wettbewerbsvorteils durch die Geheimhaltung, etwaige Schwierigkeiten der Geheimhaltung sowie die konkrete Gefährdungslage. Weiters spielen die Unternehmensgröße und die Leistungsfähigkeit eines Unternehmens, die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen, die Art der Kennzeichnung der Informationen und vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern eine Rolle.[22] Ein weiteres Kriterium bildet die

Branche, in der das Unternehmen tätig ist, da branchenüblichen Sicherheitsstandards einen wichtigen Anhaltspunkt für die Angemessenheit von Geheimhaltungsmaßnahmen darstellen.[23] Nicht gefordert werden können Geheimhaltungsmaßnahmen, die den Wert des Geschäftsgeheimnisses für das Unternehmen übersteigen[24].

3.2. Mehrfache Umgehung von Sicherheitsvorkehrungen
In einem Fall hatte das OLG Hamm[25] zu beurteilen, ob Geheimhaltungsmaßnahmen für Stopfaggregate, die für den Einsatz in Gleisstopfmaschinen entwickelt wurden, ausreichend waren. Dieses gelangte zu dem Ergebnis, dass die getroffenen Sicherungsmaßnahmen (EDV-Sicherheitsrichtlinie, reglementierter Zugriff zum sog. PZA und Geheimhaltungsvereinbarungen mit Lizenznehmern) nicht ausreichend waren, weil die getroffenen Sicherheitsvorkehrungen zu nicht näher feststellbaren Zeitpunkten in der Vergangenheit mehrfach umgangen wurden, ohne dass das Unternehmen angemessen darauf reagiert hatte und deutliche Anhaltspunkte für eine unzureichende Sicherung hatte. Die Sorglosigkeit eines Unternehmens trotz vorhandener technischer Sicherungsmaßnahmen kann zum Verlust eines Geschäftsgeheimnisses führen. Wenn es der Berechtigte duldet, dass Sicherheitsvorschriften umgangen werden, ist er demnach nicht schutzwürdig.

3.3. Wirtschaftliche Bedeutung des Geschäftsgeheimnisses
Zur Wahrung des in den Plänen liegenden Geschäftsgeheimnisses ist ein hohes Maß an Sicherheitsvorkehrungen erforderlich.[26] Weiters war relevant, dass es sich bei den Stopfaggregaten um das „Flaggschiff“ des Unternehmens handelte. Bei einem weltweit agierenden Unternehmen mit erheblicher Bedeutung am Markt ist eine höhere Anforderung zu stellen als bei kleineren Unternehmen.

3.4. Zulassen von Speichern auf privaten Datenträgern
Das OLG Stuttgart[27], hat zu Rezepturen bei Polyurethan-Schaumsystemen sowie Klebstoffen betreffenden Fall das Dulden des Speicherns von Dateien mit Geschäftsgeheimnissen auf privaten Datenträgern als äußerst kritisch angesehen, insbesondere wenn die Dateien dort ohne Passwort zugänglich sind. Dem kann jedenfalls gefolgt werden.
Papierdokumente mit Geschäftsgeheimnissen müssen gegen den Zugriff unbefugter Personen gesichert sein. Die Stellen im Unternehmen, an denen die Dokumente verwahrt werden, müssen hinreichend gegen den Zutritt unbefugter Personen gesichert sein, bei sensiblen Informationen müssen die Geheimnisse verschlossen oder der Raum abgeschlossen werden[28]. Die Umsetzung eines „need-to-know“-Prinzips im Rahmen eines Maßnahmenkonzepts ist demnach unverzichtbar.

4. Fazit
Auch, wenn die Frage was unter den Umständen angemessene Geheimhaltungsmaßnahmen zu verstehen ist, bei erster Betrachtung schwer beurteilbar ist, so zeigen die bisher dazu ergangenen Entscheidungen, dass die Gerichte zwar konsequente Maßnahmen von den Unternehmen erfordern ohne den Sorgfaltsmaßstab allzu zu überspannen. Es bleibt zu hoffen, dass mit Augenmaß praxisnahe Einzelfallentscheidungen den Maßstab weiter präzisieren. Denn ohne die Geheimnisschutzregeln können vertrauliche Informationen kaum gegenüber Dritten verteidigt werden. Der OGH geht zwar grundsätzlich davon aus, dass vertrauliche Informationen auch urheberrechtlich geschützt sein können,[29]

allerdings nur sehr eingeschränkt. Genießen Kundendaten mangels Geheimhaltungsmaßnahmen keinen Schutz nach dem UWG, können nur betroffene Personen gemäß Art 4 Z 1 DSGVO – nicht aber die Unternehmen, die von der Verwendung dieser vertraulichen Informationen betroffen sind – die unzulässige Verarbeitung ihrer personenbezogene Daten geltend machen.[30]

Korrespondenz:
RA Dr. Georg Bruckmüller, Gründungspartner der Bruckmüller Rechtsanwaltsgmbh,
georg.bruckmueller@bruckmueller-law.at

---

[1] BGBl 2018/109.

[2] § 26b UWG wurde in Umsetzung der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8.Juni 2016 über den Schutz von vertraulichen Know-Hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung formuliert.

[3] Im Sinne des § 26b Abs 1 Z 3 UWG.

[4] Im Sinne § 26b Abs 1 Z 2 UWG.

[5] Im Sinne des § 26 h UWG.

[6] Nach § 26 i UWG.

[7] OGH 19.11.2024, 4 Ob 195/24s = ZIIR-Slg 2025/19.

[8] Wie auch in dem in OGH 4 Ob 195/24s zugrunde liegenden Fall.

[9] Hofmarcher, Das Geschäftsgeheimnis (2020), Rz 2.36.

[10] Hofmarcher, Das Geschäftsgeheimnis (2020), Rz 2.38 mwN.

[11] Ebenso Rassi, Kooperation und Geheimnisschutz bei Beweisschwierigkeiten im Zivilprozess (2020), Rz 219.

[12] OGH 19.11.2024, 4 Ob 195/24s = ZIIR-Slg 2025/19.

[13] Mit Hinweis auf Thiele in Wiebe/Kodek, UWG § 26b Rz 21.

[14] OGH 19.11.2024, 4 Ob 195/24s [15] = ZIIR-Slg 2025/19.

[15] Hofmarcher, Das Geschäftsgeheimnis (2020), Rz 2.33.

[16] OGH 19.11.2024, 4 Ob 195/24s [14].

[17] OGH 19.11.2024, 4 Ob 195/24s [15].

[18] So etwa zur deutschen Rechtslage: BAG vom 17.10.2024 – 8 AZR 172/23.

[19] LAG Köln, Urteil 02.12.2019, Az 2 SaGa 20/19.

[20] OGH 19.11.2024, 4 Ob 195/24s [16] in Bezug auf das Urheberrecht.

[21] OLG Hamm 15.07.2020, 4 U 177/19 unter Hinweis auf Ohly in GRUR 2019, 441 (443).

[22] LArbG Baden-Württemberg, Urteil vom 18.08.2021, Az 4 SaGa 1/21; Ohly, GRUR 2019, 441 (444).

[23] Alexander in Köhler/Bornkamm/Feddersen UWG, 40. Auflage, § 2 GeschGehG Rn 67 f.

[24] OLG Hamm 15.07.2020, 4 U 177/19.

[25] OLG Hamm 15.07.2020, 4 U 177/19.

[26] OLG Hamm 15.07.2020, 4 U 177/19.

[27] OLG Stuttgart 19.11.2020, 2 U 575/19.

[28] Maaßen, GRUR 2019, 357 f.

[29] So auch der OGH 19.11.2024, 4 Ob 195/24s [18].

[30] Bruckmüller, Anm zu 6 Ob 132/21m „Klientendaten“ in ZIIR 2022/1, 80.
Externe Verzeichnisse: https://doi.org/10.33196/ziir202502013501
