Know-how-Schutz

Information zum Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

Thomas Becker
David Ziegelmayer
LEXANTIS Rechtsanwälte

Juli 2021

Inhalt

Kontakt

David Ziegelmayer
Rechtsanwalt, Fachanwalt für gewerblichen Rechtsschutz

Hohenzollernring 57
50672 Köln

T +49 221 467 835 20
F +49 221 467 835 21
M +49 163 427 80 49
E david.ziegelmayer@lexantis.com

Thomas Becker, LL.M. Eur.
Rechtsanwalt

www.lexantis.com

T +49 221 467 835 10
F +49 221 467 835 11
M +49 173 20 97 898
E thomas.becker@lexantis.com

„He that would keep a secret must keep it secret that he hath a secret to keep."

Francis Bacon

„Unternehmen nutzen Geschäftsgeheimnisse unabhängig von ihrem Betätigungsfeld oder ihrer Größe, oftmals ohne dass sie sich selbst ihrer Abhängigkeit von diesen immateriellen Werten bewusst sind. In diesem Umfeld hat eine sehr große Anzahl der Unternehmen aller Industriezweige pragmatisch den ältesten und offensichtlich einfachsten Mechanismus übernommen, um solche strategischen Werte zu schützen: Sie behalten ihre Geschäftsgeheimnisse für sich."

EU-Kommission, "Study on Trade Secrets and Business Information in the Internal Market", S. 1

„Erfüllungsaufwand für die Wirtschaft
Ein gewisser Erfüllungsaufwand kann sich daraus ergeben, dass Unternehmen angemessene Maßnahmen zum Schutz von Geschäftsgeheimnissen treffen müssen, um in den Schutzbereich des Entwurfs zu fallen. Der hierfür anfallende Erfüllungsaufwand kann nicht geschätzt werden, weil die angemessenen Maßnahmen abhängig von der Art des Geschäftsgeheimnisses und des Unternehmens sehr unterschiedlich sein können."

Referentenentwurf
des Bundesministeriums der Justiz und für Verbraucherschutz
Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 (Stand 28.03.2018)

Einführung

Der Schutz von Geschäfts- und Betriebsgeheimnissen ist seit jeher von besonderer Bedeutung für Unternehmen. Die Gefährdungsszenarien sind vielfältig. Eine konstante Gefahr geht in Unternehmen von eigenen Mitarbeitern oder engen geschäftlichen Partnern aus, die unmittelbar Zugriff auf die Betriebsgeheimnisse des Unternehmens erhalten. Die Digitalisierung hat zusätzlich dazu geführt, dass Informationen komprimiert auf kleinem Raum und häufig (fast) unbemerkt aus dem Unternehmen hinausgetragen werden können. Schon immer gab es das Phänomen der Betriebsspionage von Außen. Die Virtualisierung, Vernetzung und die Nutzung des Internets als Transportmedium für Unternehmensinformationen führen dazu, dass gezielte Betriebsspionage oder andere Formen des kriminellen Zugriffs auf Unternehmensinformationen „aus der Ferne" möglich werden. Unternehmen und Behörden verzeichnen in den letzten Jahren einen erheblichen Anstieg der Betriebsspionage und Cyberkriminalität.

Auf nationaler Ebene gab und gibt es unterschiedlichste Rechtsinstrumente zum Geheimnisschutz. Im Jahr 2016 ist daher der Europäische Gesetzgeber aktiv geworden und hat mit der *EU-Richtlinie 2016/943 vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung*[1] („Richtlinie") den Versuch unternommen, einheitliche europäische Standards zum Schutz von Unternehmensgeheimnissen festzulegen. Die Richtlinie war bis zum **9. Juni 2018** in nationales Recht umzusetzen.

Der Deutsche Bundestag hat – mit reichlich „Verspätung" – am 21.03.2019 *ein neues Stammgesetz („Gesetz zum Schutz von Geschäftsgeheimnissen – **GeschGehG**")* beschlossen[2]*, das die Richtlinie in der Bundesrepublik* umsetzt. Es ist **am 25. April 2019 in Kraft getreten**. Mit dem Gesetz wird letztlich eine Angleichung des Geheimnisschutzes an „klassische" Immaterialgüterrechte erfolgen. Auch vor dem in Kraft treten des Gesetzes *mussten die Gerichte die nationalen Regelungen seit 10. Juni 2018 aber in jedem Fall zwingend richtlinienkonform auslegen*.

Diese Normen stellen den Begriff des „Geschäftsgeheimnisses" (engl. „trade secret", frz. „secret d'affaires") ins Zentrum ihres Regelungsansatzes. In der Literatur ist der Einfachheit halber häufig von „Know-how" und entsprechend von der „Know-how"-Richtlinie" die Rede. *Wir verwenden den Begriff des „Know-how" auch in diesem Dokument als Oberbegriff für Geschäfts- und Betriebsgeheimnisse*.

Das Kernprinzip des Geheimnisschutzes ist, dass sensible Informationen dann aber auch nur dann rechtlich geschützt ist, wenn sie vom Berechtigten durch „angemessene Geheimhaltungsmaßnahmen" geschützt und geheim gehalten wird, § 2 GeschGehG. Dies kann und sollte durch faktische Maßnahmen ebenso wie durch die (vertrags-)rechtliche Absicherung sensibler Informationen geschehen.

Mittlerweile liegen erste obergerichtliche Entscheidungen zur Auslegung des GeschGehG vor. Dabei zeigt sich, dass die Gerichte durchaus in der Regel nur dann gewillt sind, einen effektiven Rechtsschutz zu gewähren, wenn sich Unternehmen um ihre Geheimnisse „kümmern". Das bedeutet z.B., dass in Anbetracht der Bedeutung des Geschäftsgeheimnisses jedem Hinweis auf eine Verletzung sorgfältig nachzugehen ist und ein vorhandenes Sicherheitskonzept wenn nötig zeitnah anzupassen ist.

Die Regelung des Know-how-Schutzes durch die Richtlinie ist keinesfalls eine europäische Sonderregelung. Der Schutz von „Trade Secrets" war bereits Gegenstand des sog. TRIPS-Abkommens, das 1994 als Teil der WTO-Verträge verabschiedet wurde[3]. Fast zeitgleich mit dem Erlass der Richtlinie haben die USA mit dem „Defend Trade Secrets Act" im April 2016 ebenfalls ein Gesetz zum Schutz von Geschäftsgeheimnissen auf den Weg gebracht.[4]

Dieses Dokument gibt einen kurzen Überblick über den Inhalt des Gesetzes, angemessenen Schutzmaßnahmen im Allgemeinen, Vertraulichkeitsvereinbarungen im Besonderen und die Rechtsschutzmöglichkeiten nach der Richtlinie. Das Dokument dient der allgemeinen Information und ersetzt nicht die Rechtsberatung im Einzelfall.

---

[1] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L0943
[2] http://dipbt.bundestag.de/extrakt/ba/WP19/2385/238528.html
[3] https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm#7
[4] https://www.gpo.gov/fdsys/pkg/PLAW-114publ153/html/PLAW-114publ153.htm

Die Know-how-Richtlinie und das GeschGehG

Ziele

Ziel der Gesetzgebung ist die Schaffung eines einheitlichen Niveaus beim Know-how- bzw. Geheimnisschutz und vor allem bei dessen gerichtlicher Durchsetzung. Bislang sind die Unterschiede bei der Rechtsdurchsetzung innerhalb der EU[5] bzw. des EEA erheblich. Teilweise gibt es zivilrechtliche, teilweise nur einzelne strafrechtliche Sanktionen. Die Richtlinie zielt daher auf eine zivilrechtliche Rechtsvereinheitlichung in Bezug auf folgende Aspekte:

- Wirksamer Schutz vor widerrechtlicher Aneignung
- Effektive Rechtsbehelfe im Verletzungsfall
- Schutz der Vertraulichkeit in Gerichtsverfahren

Definition von Know-how und Geschäftsgeheimnissen

Know-how bzw. Geschäftsgeheimnis ist nach Art. 2 Nr. 1 (c) der Richtlinie und nach dem § 2 Nr. 1 GeschGehG eine Information, die *kumulativ* die nachstehenden Kriterien erfüllt:

- sie ist *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* und daher von wirtschaftlichem Wert
- sie ist ***Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen*** durch ihren rechtmäßigen Inhaber ist und
- es besteht ein *berechtigtes Interesse an der Geheimhaltung* (*hier geht das GeschGehG über die RiLi hinaus*).

Die Definition entspricht im Wesentlichen derjenigen, die schon 1994 in Art. 39 des TRIPS-Abkommens verwendet wurde. Der Know-how-Begriff ist damit im Ansatz denkbar weit. Mit dem weiten Begriff möchte die Richtlinie praktisch jede Form „intellektuellen Kapitals" schützen. In den Erwägungsgründen der Richtlinie wird klargestellt, dass ein breites Spektrum von Informationen geschützt werden soll, das über technologisches Wissen (Know-how im engeren Sinne) hinausgeht und auch Geschäftsideen wie Informationen über Kunden und Lieferanten, Businesspläne sowie Marktforschung und -strategien umfasst.

„Know-how" wird zwar auch als Sammelbegriff verwendet. Herkömmlich versteht man aber unter Know-how vor allem technisches Wissen beispielweise in Bezug auf Fertigungs- und Herstellungsmethoden. Die Begriffe „Geschäftsgeheimnis" und „Betriebsgeheimnis" sind weiter zu verstehen, sie gehen über das technische Wissen hinaus und umfassen jedes kaufmännisch oder unternehmerisch relevante Sonderwissen. In diesem Sinne stellt Know-how in der Regel ein Geschäftsgeheimnis dar, aber nicht jedes Geschäftsgeheimnis besteht aus technischem Know-how.

Beispiele

Forschung und Entwicklung
Erfindungen, Designs, Konstruktionszeichnungen, Zusammensetzungen, Rezepturen, Eigenschaften von Produkten und Komponenten

Herstellung, Leistungserbringung
Spezifikationen, Anforderungen, Fertigungsverfahren, Testverfahren, Vorgehensmodelle, Kapazitäten, Einzelkosten, Kostenstrukturen, Löhne & Gehälter

Einkauf
Bezugsquellen, Lieferanten, Preise, Konditionen, Kalkulationsgrundlagen

Verkauf, Marketing
Kundendaten, Preise, Vertriebswege, Distributoren, Marktanalysen, Verbraucherverhalten, Kundenwünsche, Logistikinformationen

Unternehmensstrategie
Geschäftsmodelle, Personalien, Innovationen, Business-Pläne, Investitionspläne, Marketing-Pläne

Transaktionen, Wachstum
Fusionspläne, Verkaufs- und Kaufabsichten, Expansionspläne, Inhalt und Ablauf von M&A-Verhandlungen, Marktentwicklung

IT
Systemarchitektur, Eigenentwicklungen, Sourcecode, Algorithmen, Inhaltsdaten, Metadaten, Big Data-Analysen

[5] s. zum Status Quo der Rechtsdurchsetzung in der EU die Studie des EUIPO (2018), https://bit.ly/2wljCVo

Wesentliche Neuerungen

Erfordernis „angemessener Geheimhaltungsmaßnahmen“

Die gesetzgeberischen Tendenzen der vergangenen Jahre legen den Fokus zunehmend auf die Maßnahmen, die Unternehmen *selbst* zum Schutz ihres Know-how ergreifen. Auch nach der Richtlinie und dem GeschGehG unterliegt daher jedes Geheimnis „*den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen*“. Fehlt es an solchen Maßnahmen, fällt die konkret betroffene Information bereits aus der Definition des „Geheimnisses“ heraus.

Dies hat in Deutschland bereits zu einer Verschärfung der Anforderungen an den Schutz von Geheimnissen führen, weil deren Definition „enger“ wird. Die frühere deutsche Rechtsprechung, die nach dem bis April 2019 geltenden § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) bislang keine hohen Anforderungen an den Geheimnisschutz, insbesondere an den (subjektiven) Willen zur Geheimhaltung stellte, steht im Widerspruch zu dem objektiven Erfordernis „*angemessener Geheimhaltungsmaßnahmen*“ aus dem GeschGehG.

***Grundprinzip:* Keine Schutzmaßnahme - kein Geheimnis!**
Art. 2 Nr. 1 (b) der Richtlinie 2016/943, § 2 Nr. 1 GeschGehG

[Geschäftsgeheimnisse]
„…sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen“

Welche Maßnahmen als geeignet und vor allem als „angemessen“ anzusehen sind, ist dem GeschGehG nicht unmittelbar zu entnehmen. In der Rechtsprechung[6] wird z.B. gefordert, dass relevante Informationen nur Personen anvertraut werden dürfen, die die Informationen zur Durchführung ihrer Aufgabe (potentiell) benötigen und die zur Verschwiegenheit verpflichtet sind. Vor dem Hintergrund, dass der Geheimnisschutz vor allem durch das TRIPS-Abkommen international abgesichert wird, sind hinsichtlich der Angemessenheit auch ausländische und internationale Gepflogenheiten und Rechtstraditionen, insbesondere aus dem angloamerikanischen Raum, zu berücksichtigen. Internationale „Best Practice“-Ansätze lassen sich sehr weitgehend auch für innerstaatliche Sachverhalte nutzen. Siehe dazu die → *Darstellung der vertraglichen Schutzmechanismen und des Schutzkonzepts (unten)*.

Geheimnisschutz im Prozess

Die „*angemessenen Geheimhaltungsmaßnahmen*“ sind nach der Richtlinie eine wesentliche Bedingung für die Inanspruchnahme effektiver Rechtsbehelfe, die aufgrund der Richtlinie durch innerstaatliche Regelungen einzurichten sind. Unter dem Eindruck des TRIPS-Abkommens und nunmehr der Richtlinie haben die Gerichte bereits damit begonnen, nationale Regelungen zum Geheimnisschutz völkerrechts- und richtlinienkonform auszulegen. In Geheimnisschutzprozessen fragen Gerichte zunehmend danach, *welche konkreten Maßnahmen das Schutz suchende Unternehmen getroffenen hat, um behauptetes Know-how zu schützen*. Es ist abzusehen, dass sich dieser Ansatz verfestigen wird. Unternehmen, die sich in Gerichtsverfahren erfolgreich auf Regelungen zum Geheimnisschutz berufen wollen, werden nach der Richtlinie künftig zwingend darlegen müssen, welche konkreten „Maßnahmen“ sie zum Schutz ihrer Geheimnisse ergriffen haben. Sind sie dazu nicht in der Lage, droht der Prozessverlust.

Aktuelle Beispiele aus der Rechtsprechung (US/DE)
Zit. Berkley Risk Administrators./. Accident Fund Holdings, Civ. No. 16-2671, 24.08.2016:
„serious questions as to whether [plaintiff] ***took reasonable efforts to maintain the secrecy of the information at issue“***
OLG Hamburg (Beschwerdebeschluss 2017):
„Ob und wie die Entwicklungsarbeiten und -ergebnisse geheim gehalten worden sind und ob nur ein eng begrenzter Personenkreis Zugriff hatte, steht damit nicht fest.“

Zu beachten ist in diesem Zusammenhang die „Whistleblowing-Richtlinie“[7], nach der Arbeitnehmer in Gerichtsverfahren wegen Verleumdung, Verletzung des Urheberrechts, Verletzung der Geheimhaltungspflicht, Verstoßes gegen Datenschutzvorschriften, Offenlegung von Geschäftsgeheimnissen sowie Schadensersatzverfahren aufgrund von „Whistleblowing“ in keiner Weise haftbar gemacht werden können. Diese Personen haben das Recht, unter Verweis auf die betreffende Meldung oder Offenlegung die Abweisung der Klage zu beantragen, sofern sie hinreichenden Grund zu der Annahme hatten, dass die Meldung oder Offenlegung notwendig war, um einen Verstoß gemäß der Richtlinie aufzudecken.

Diejenigen Unternehmen, die ein wirksames Schutzkonzept für ihre Geheimnisse umgesetzt haben und hinreichend nachweisen können, kommen nach Umsetzung der Geheimnisschutz-Richtlinie aber in der Regel in den Genuss einer *EU-weiten Stärkung der prozessualen Vorschriften zum Geheimnisschutz*.

[6] OLG Stuttgart, Urt. v. 19. November 2020, 2 U 575/19 –Schaumstoffsysteme
[7] (EU) 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, https://bit.ly/2YFC3DC

Das GeschGehG sieht etwa Vorschriften zur Wahrung der Vertraulichkeit von Geschäftsgeheimnissen im Verlauf von Gerichtsverfahren vor, bei denen der rechtswidrige Erwerb oder die rechtswidrige Nutzung oder Offenlegung eines Geschäftsgeheimnisses Gegenstand des Verfahrens ist:

- Dazu zählt die Möglichkeit, den *Zugang zu von den Parteien oder Dritten vorgelegten Dokumenten, die Geschäftsgeheimnisse oder angebliche Geschäftsgeheimnisse enthalten, ganz oder teilweise auf eine begrenzte Anzahl von Personen zu beschränken*, §§ 16 ff. GeschGehG. Das GeschGehG geht in den Schutzmaßnahmen noch über die Richtlinie hinaus und sieht in § 17 ff. z.B. Ordnungsgelder für den Fall der Verletzung der Vertraulichkeit im Prozess vor.

- Ebenso können Gerichte eine *„nicht vertrauliche" Fassung einer gerichtlichen Entscheidung* bereitstellen, in der die Geschäftsgeheimnisse enthaltenden Passagen gelöscht oder geschwärzt wurden.

Zu weiteren Aspekten der → *Rechtsdurchsetzung* siehe unten.

Verschärfung der Rechtsfolgen

Die Art. 10 bis 15 der Richtlinie und § 6 ff. des GeschGehG regeln die Rechtsfolgen der Geheimnisverletzung und unterscheiden dabei zwischen vorläufigen Maßnahmen, die ein Gericht anordnen können muss und Maßnahmen aufgrund einer Sachentscheidung.

- Besonders scharfe Maßnahmen sind für den Fall vorgesehen, in dem z.B. ein Unternehmen Dienstleistungen oder Produkte auf den Markt bringt, die auf Geschäftsgeheimnissen eines Wettbewerbers beruhen (§ 7 GeschGehG). Hier kann ein Gericht die *Vernichtung* der Gesamtheit oder eines Teils der Dokumente, Gegenstände, Materialien, Stoffe oder elektronischen Dateien anordnen, die das Geschäftsgeheimnis enthalten. Auch der *Rückruf der rechtsverletzenden Produkte vom Markt* ist als Sanktion ausdrücklich vorgesehen. Das GeschGehG sieht zudem auch noch auch Auskunfts- und Schadensersatzansprüche, sowie die persönliche Haftung des Unternehmensinhabers vor (§ 12).

- Art. 14 regelt die Schadensersatzverpflichtung des Schädigers, die in § 10 des GeschGehG umgesetzt wird. Das Gericht kann auf Antrag des Geschädigten anordnen, dass ein Rechtsverletzer, der wusste oder hätte wissen müssen, dass er einen rechtswidrigen Erwerb oder eine rechtswidrige Nutzung oder Offenlegung eines Geschäftsgeheimnisses vornahm, dem Inhaber des Geschäftsgeheimnisses Schadensersatz leistet. In der Bundesrepublik hatte die Rechtsprechung die Rechtsfolgen einer Geheimnisverletzung den Immaterialgüterrechten, für die ähnliche Vorgaben aufgrund der Enforcement-RL 2004/48/EG gelten, bereits angenähert. So ist etwa im Bereich des Geheimnisschutzes nach dem deutschen UWG die Möglichkeit der dreifachen Schadensberechnung anerkannt.

Zulässigkeit des Reverse Engineering

Eine wesentliche Neuerung für das deutsche Recht ergibt sich aus § 3 Abs. 1 Nr. 2 GeschGehG schließlich für das sog. Reverse Engineering, also für die Informationsgewinnung durch „Rückentwicklung" oder sonstige genaue Untersuchung von Produkten oder Gegenständen von Wettbewerbern.

Ein solches Vorgehen zur Erlangung geheimer Informationen galt bislang in Deutschland in vielen Fällen als unlauter und damit als unzulässig. Die *Richtlinie sieht es demgegenüber ausdrücklich als zulässiges Mittel des Wettbewerbs an und erklärt das Reverse Engineering für rechtmäßig*. Dies gilt jedenfalls dann, wenn die untersuchten Produkte rechtmäßig erworben wurden oder der jeweilige Gegenstand öffentlich verfügbar gemacht wurde.

Es bleibt damit nur die Möglichkeit, das → *Reverse Engineering im Einzelfall vertraglich zu beschränken (s. Beispiel im Anhang).*

BGH vs. Richtlinie

BGH GRUR 1980, 750, 751:

„Daß von der bekannten Rezeptur Hinweise ausgehen, die es […] ermöglichen, […] ein dem Lizenzgegenstand ebenbürtiges Medikament zu entwickeln, nimmt allein weder dem Präparat - also dem Erzeugnis - noch dem Herstellungsverfahren den Geheimnischarakter"

Art. 3 Abs. 1 (b) Richtlinie, § 3 Abs. 1 Nr. 2 GeschGehG:

„…Ein Geschäftsgeheimnis darf insbesondere erlangt werden durch ***[…] Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der öffentlich verfügbar gemacht wurde oder sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt"***

Vertraglicher Know-how-Schutz

Schutz über vertragliche Regelungen essenziell

Auch und gerade unter Geltung des GeschGehG bleibt es dabei: Der Schutz von Know-how/Geschäftsgeheimnissen ist vor allem über vertragliche Regelungen zu erreichen, etwa durch Vertraulichkeitsvereinbarungen.
Art. 4 Abs. 3 (c) der Richtlinie und § 4 Abs. 2 GeschGehG erklären den Verstoß gegen derartige Vereinbarungen ausdrücklich zu einer rechtswidrigen Handlung. Mit anderen Worten: Nur mit einer *wirksamen* Vertraulichkeitsvereinbarung werden Nutzung und Erwerb von Geschäftsgeheimnissen in vielen Fällen künftig überhaupt erst rechtswidrig. Eine Vertraulichkeitsvereinbarung ist damit eine von vielen „angemessenen Geheimhaltungsmaßnahmen" im Sinne des GeschGehG.

Vertraulichkeitsvereinbarungen mit Dritten (NDAs)

Die größte Relevanz kommt im vertragsrechtlichen Bereich den *Vertraulichkeitsvereinbarungen* („Non Disclosure Agreement" – NDA) zu. Durch sie wird sichergestellt, dass insbesondere Dienstleister, Subunternehmer, Lieferanten sowie Partner in Kooperations- und Entwicklungsprojekten, denen im Laufe der Zusammenarbeit vertraulichen Informationen bekannt werden, diese nur zu den vertraglich festgelegten Zwecken nutzen dürfen. Ziel ist es, ihnen nur ein möglichst eng begrenztes minimales „Nutzungsrecht" hinsichtlich bereitgestellter Informationen einzuräumen und sie dazu zu verpflichten, ihrerseits angemessene Geheimhaltungsmaßnahmen zu treffen. Dazu gehört in besonderem Maße die Kontrolle eigener Mitarbeiter und der Mitarbeiter von Erfüllungsgehilfen oder Subunternehmen beim Umgang mit vertraulichen Informationen des Vertragspartners.

Die entsprechenden Regelungen können *entweder Bestandteil der jeweiligen Hauptverträge sein oder in selbstständigen NDAs vereinbart* werden. Selbstständige NDAs werden dabei vor allem im Vorfeld vor Abschluss weitergehender Leistungs- oder Austauschverträge geschlossen, um den für die Vorbereitung des beabsichtigten Hauptvertrags notwendigen Informationsaustausch abzusichern. Dabei ist es wichtig, darauf zu achten, dass das NDA entweder auch nach Abschluss des Hauptvertrags weiterhin gilt oder eindeutig durch entsprechende Regelungen im Hauptvertrag abgelöst wird.

Da NDAs von Unternehmen oft in großer Zahl abgeschlossen werden, um den Informationsschutz in jeder Hinsicht zu gewährleisten, hat sich ein sehr hohes Maß an *Standardisierung von NDAs* herausgebildet. Insbesondere die Festlegungen, wann Informationen nicht als geheim anzusehen sind und wann an sich geheime Informationen ausnahmsweise gegenüber Dritten offenbart werden dürfen (z.B. zur Erfüllung gesetzlicher, behördlicher oder gerichtlicher Offenlegungspflichten), folgen einem weitgehend einheitlichen Muster. Die entsprechenden Ausnahmefälle sind trotzdem sorgfältig auf die besonderen Gegebenheiten des jeweiligen Unternehmens abzustimmen, um nicht versehentlich Schlupflöcher zu gewähren. Auch Löschungs- bzw. Rückgabepflichten bei Beendigung des Vertragsverhältnisses sind sorgfältig zu formulieren. Die Regelungen sollen sowohl klar und einfach in ihrer Durchsetzung sein, darüber hinaus aber auch praktikabel und rechtlich erfüllbar sein. Insbesondere müssen Unternehmen ihren gesetzlichen Aufbewahrungspflichten genügen. Sie können und sollen aber nicht gezwungen werden, technisch oder wirtschaftlich unsinnigen Aufwand zu treiben, um einzelne Informationen zu isolieren und zu löschen. Für *digitale Informationen* sollte daher festgelegt werden, wie mit Kopien in Backups und Archiven umzugehen ist. Ist eine Löschung zwar technisch möglich, aber unverhältnismäßig aufwendig, empfiehlt sich als Kompromisslösung eine Ausnahme für die Löschungspflicht, aber gleichzeitig eine Verlängerung der Geheimhaltungspflicht – ggf. auf unbeschränkte Zeit.

Muster-NDAs sollten vor dem Hintergrund der Richtline überprüft werden. Vor allem der Konkretisierung des Schutzgegenstandes und des Schutzumfangs in Bezug auf den jeweiligen Vertragszweck dürfte künftig größere Bedeutung zukommen, wenn die Gerichte detaillierter prüfen, ob gerade in Bezug auf die konkrete, streitbefangene Information angemessene Schutzmaßnahmen bestanden haben. Es empfiehlt sich, die allzu verbreitete Nutzung von „globalen" oder „general purpose"-NDAs zu hinterfragen. Die Verantwortlichen im Unternehmen sind für das Thema zu sensibilisieren – etwa durch Schulungen oder Informationsveranstaltungen. Die Prozesse zum Abschluss von NDAs sollten so aufgesetzt sein, dass unter Einschaltung der Rechtsabteilung oder anderer, geschulter Personen jeweils rechtzeitig sinnvolle und konkrete NDAs abgeschlossen werden.

Vereinbarungen mit Arbeitnehmern

Besondere Maßnahmen im Verhältnis zu Mitarbeitern des Unternehmens sind unabdingbar, um für einen „angemessen" Geheimnisschutz im Sinne der Richtlinie und des GeschGehG zu sorgen. Grundsätzlich geht das Arbeitsrecht von bestimmten Loyalitätspflichten des Mitarbeiters aus, zu denen auch – unausgesprochen – die Verpflichtung gehört, Geschäfts- und Betriebsgeheimnisse des Arbeitgebers zu wahren. Fraglich ist, welche Maßnahmen darüber hinaus notwendig sind. Im Rahmen der Umsetzung der Richtlinie hat der deutsche Gesetzgeber hier nicht unbedingt mehr Klarheit

geschaffen. Die Unternehmen sind also gehalten, sich die Frage selbst zu beantworten, solange die Rechtsprechung keine klaren Leitlinien entwickelt hat. Hilfreich kann auch hier die Rechtsprechung zu „angemessenen Geheimhaltungsmaßnahmen“ aus Rechtsordnungen sein, die mit diesem Merkmal bereits länger umgehen. Nach der Rechtsprechung US-amerikanischer Gerichte etwa

- müssen jedenfalls die einmal als angemessen empfundenen Maßnahmen und das damit erreichte Schutzniveau dauerhaft aufrechterhalten werden.
- muss das geheime Know-how im Unternehmen auch faktisch als Geheimnis behandelt werden. Arbeitnehmer müssen demnach auf das Vorliegen von Geschäfts Geheimnissen besonders hingewiesen werden und die Zugriffe auf eine „Need to know“-Basis beschränkt sein.
- müssen sich die Maßnahmen zudem konkret auf die jeweiligen Geheimnisse beziehen.

Neben *arbeitsvertraglichen oder separaten Vertraulichkeitsregelungen* etwa im Zusammenhang mit besonderen Projekten ist es daher auch notwendig, die hinreichenden Kenntnisse und das richtige Bewusstsein im Unternehmen für den Geheimnisschutz sicherzustellen: Personen, die mit sensiblen Informationen zu tun haben, sollten daher zwingend zur Klassifizierung und Kennzeichnung von sensiblen Informationen sowie in Bezug auf den Umgang mit konkreten Geheimnissen geschult werden. Dasselbe gilt für Rückgabepflichten von Dokumenten und Dateien sowie Folgen von Geheimnisverwertungen nach Beendigung des Arbeitsverhältnisses[8].

Im Mindestmaß ist also sicherzustellen, dass Mitarbeiter *vertraglich für die Zeit während und nach dem Arbeitsverhältnis zur Verschwiegenheit in Bezug auf die Geschäftsgeheimnisse des Arbeitgebers verpflichtet werden.* Dies sollte grundsätzlich schon im Arbeits- oder Anstellungsvertrag erfolgen, lässt sich aber auch noch später nachholen, z.B. im Rahmen eines Aufhebungsvertrags (siehe Beispiele → *im Anhang*). Solche nachträglichen Vereinbarungen sind nach Auffassung des BAG auch ohne Karenzentschädigung regelmäßig wirksam, wenn sie sich auf bestimmte Geheimnisse beschränken und den Arbeitnehmer nicht in seinem beruflichen Fortkommen einschränken.

Faustregel:
Was der Arbeitnehmer „im Kopf“ hat, darf er grundsätzlich überall hin „mitnehmen“!
Ausnahmen gelten (nur) dann, wenn wirksam eine auf das konkrete Geheimnis Verschwiegenheitsvereinbarung getroffen und/oder oder ein Wettbewerbsverbot vereinbart wurde

Hingegen verbieten sich *nachvertragliche Schweigepflichten*, die sich nicht auf ein oder mehrere konkret festgelegte Betriebsgeheimnisse, sondern unterschiedslos auf alle Geschäftsvorgänge beziehen, so dass dem Arbeitnehmer bei weiter Auslegung letztlich jede berufliche Verwertung seines Erfahrungswissens untersagt würde. Derartige Regelungen dürften meist unwirksam sein[9]. Wird ein Geschäftsgeheimnis nicht konkret bezeichnet, kann eine unwirksame Geheimhaltungsklausel vorliegen, an die sich der Mitarbeiter nach Beendigung des Arbeitsverhältnisses nicht halten muss. In einem solchen Fall kann es mangels wirksamer Geheimhaltungspflichten an einer „angemessenen Geheimhaltungsmaßnahme“ im Sinne der Richtlinie fehlen.

Ein praktisch wichtiger Aspekt des Geheimnisschutzes ist die Frage, ob ein Mitarbeiter in einem kritischen Bereich im Fall einer Kündigung noch faktisch die Möglichkeit hat, Unternehmensgeheimnisse „beiseite zu schaffen“. Erfahrungsgemäß finden Geheimnisschutzverletzungen besonders häufig in dieser letzten Phase eines Arbeitsverhältnisses statt. Im Hinblick darauf ist es gerade bei Wissensträgern im Unternehmen wichtig, im Anstellungsvertrag die Möglichkeit vorzusehen, den Arbeitnehmer während der Kündigungsfrist jederzeit unter Fortzahlung seines Gehalts freizustellen, um ihn in der „kritischen Phase“ der Beendigung vom Zugriff auf Know-how des Unternehmens fernzuhalten (siehe Beispiel → *im Anhang*).

Die Geheimhaltung bestimmter Informationen kann dem Mitarbeiter nach Ausscheiden aus seinem Arbeitsverhältnis gegen Vereinbarung einer Karenzentschädigung, zeitlich maximal befristet auf zwei Jahre auferlegt werden. Das bietet sich gerade bei solchen Mitarbeitern an, die Hauptträger von Know-how/Betriebsgeheimnissen sind. Entsprechende Verschwiegenheitsverpflichtungen werden so mit einem *Wettbewerbsverbot* gekoppelt (siehe Beispiel → *im Anhang*).

→ *s. hierzu auch Ziegelmayer u.a.: „Arbeitsrechtliche Auswirkungen der Geheimnisschutzrichtlinie“, Der Betrieb 30.09.2016, Heft 39, Seite 2295 - 2299*

[8] OLG Düsseldorf, Urt. v. 21. November 2019, I-2 U 34/19 –Spritzgießwerkzeug für Spritzen
[9] LAG Köln ArbRAktuell 2020, 395, beck-online

Rechtsdurchsetzung

Der „Diebstahl“ von Know-how wird trotz zum Teil sehr schwerwiegender wirtschaftlicher Folgen häufig nicht verfolgt. Die Gründe hierfür dürften vielfältig sein: Die strafrechtliche Verfolgung gem. §§ 17 ff. UWG a.F. (nun § 23 GeschGehG) kann aus Unternehmenssicht gravierende negative Folgen für den Betriebsfrieden oder das Betriebsklima haben. Auch wird der Gedanke einer öffentlichkeitswirksamen Verhandlung des Falles viele Unternehmen von der strafrechtlichen Verfolgung abhalten. Die Möglichkeiten einer zivilrechtlichen Verfolgung erscheinen den Unternehmen demgegenüber mühsam, kostspielig und von sehr ungewissem Ausgang. Hinzu kommt, dass Inhaber von Geschäftsgeheimnissen angesichts der vermeintlichen Gefahr der Offenbarung häufig davor zurückschrecken, ein – potenziell öffentliches – Gerichtsverfahren zum Schutz ihrer Geschäftsgeheimnisse einzuleiten.

All diese Gründe für zögerliches Verhalten sollten spätestens mit Umsetzung der Richtlinie durch das GeschGehG in den Hintergrund treten. Schon bisher zeigt die Erfahrung, dass Unternehmen, die für den drohenden „Verlustfall“ gut vorbereitet sind, auch im Zivilprozess gute Karten haben, zumindest einen weiteren Abfluss von Geschäftsgeheimnissen und Know-how zu verhindern und im günstigen Fall Rückruf- und Schadensersatzansprüche durchzusetzen. Schon unter dem Einfluss des TRIPS-Abkommens und der Enforcement-Richtlinie[10] ist das Bewusstsein der Gerichte für entsprechende Sachverhalte gestiegen und ließen sich in Verfahren gute Ergebnisse zum Geheimnisschutz erzielen. Mit den *besonders weitreichenden Maßnahmen in § 6 ff. des GeschGehG* erhalten die Gerichte nun ein weitreichendes Instrumentarium, um effizienten Geheimnisschutz sicherzustellen, sofern betroffene Unternehmen sich angemessen auf die Anforderungen des Gesetzes einstellen.

Hier sollten Unternehmen für die nachfolgend dargestellten Phasen einer Verletzung von Geschäfts-/Betriebsgeheimnissen des Unternehmens vorsorgen:

Entdeckungsphase

Da der Abfluss von Know-how in Form eines Geheimnisverrats für Unternehmen stets „überraschend“ kommt, muss schon bei der Aufdeckung eines möglichen Abflusses von Know-how ein *Notfallplan* erarbeitet sein, der zumindest zu folgenden Aspekten Festlegungen trifft:

- Zuständigkeit für die Verfolgung/Ermittlung von Informationsdiebstahl und ähnlichen Vorfällen
- Interne Berichtsketten zur Sicherstellung einer schnellen Willensbildung/Reaktion
- Externe Ressourcen (IT-Forensiker, PR-Fachleute, beratende/prozessführende Anwälte)

Das mit der Untersuchung befasste Team sollte aus speziell geschulten Personen bestehen und möglichst klein sein. Die *Einbeziehung der HR-Abteilung* ist zwingend notwendig. Zur Vermeidung von „Verdunkelungsmaßnahmen“ etwa bei einer Weitergabe von Geheimnissen an einen Wettbewerber sollte *keinesfalls eine „Anhörung“ und/oder Abmahnung der im Verdacht stehenden Person(en)* erfolgen, bevor über alle weiteren Maßnahmen entschieden ist. Bei im Verdacht von Geheimnisschutzverstößen stehenden Mitarbeitern empfiehlt sich in der Regel eine *IT-forensische Analyse der von dem Arbeitnehmer genutzten Geräte durch externe Fachleute*. Schon zur Sicherung der Beweiskraft sollte dies durch Dritte und nicht durch eigene Mitarbeiter erfolgen.

Entscheidungsphase

Nach der Sammlung, Zusammenstellung und Auswertung von Indizien muss die Entscheidung getroffen werden, ob *zivil- oder arbeitsgerichtliche Maßnahmen ergriffen und/oder Strafverfolgungsbehörden* (Geheimnisverrat = Antragsdelikt) eingeschaltet werden. Die *Zuständigkeit* der Zivil- und Arbeitsgerichte bestimmt sich u.a. danach, ob es um eine Streitigkeit „aus dem Arbeitsverhältnis“ geht, mit der Folge einer arbeitsgerichtlichen Zuständigkeit, oder ob (auch) ein Wettbewerber Geheimnisse verwertet, so dass die Sache von den ordentlichen Gerichten entschieden werden kann.

In allen Fällen ist Schnelligkeit ein oberstes Gebot und die *jeweiligen Fristen sind zu beachten*: Für einen Antrag auf Erlass einer einstweiligen Verfügung, der aufgrund des „einseitigen Verfahrens“ ohne Anhörung des Gegners erfolgen kann, besteht *Eilbedürftigkeit in der Regel nur bis maximal einem Monat nach erstmaliger Kenntnisnahme* von dem jeweiligen Vorfall. Für einen *Strafantrag in Bezug auf § 23 GeschgehG bleiben maximal drei Monate ab Kenntnis von Tat und Täter (Antragsfrist gemäß § 77b Abs. 1 S. 1 StGB)*.

[10] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014L0104

Verfolgungsphase

Um ein Verfahren erfolgreich einzuleiten, muss der Geheimnisinhaber in einer Strafanzeige oder einem Antrag auf Erlass einer einstweiligen Verfügung eine hinreichende Wahrscheinlichkeit für das Vorliegen einer Verletzung von Geheimnissen (etwa nach § 4 GeschGehG) und eine besondere Dringlichkeit glaubhaft machen[11]. Schon bei der Formulierung des jeweiligen Antrags ist – auch unter Nutzung der von der Richtlinie nunmehr vorgesehenen Möglichkeiten (s.a. § 16 ff. GeschGehG) – *darauf zu achten, die Geschäftsgeheimnisse des Geschädigten nicht zu offenbaren bzw. deren Preisgabe einzugrenzen*.

Gelingt dies, bestehen *gute Chancen für folgende Maßnahmen der Durchsetzung*:

Strafecht	Wettbewerbsrecht	Arbeitsrecht
• Durchsuchung durch die Polizei im Zuge des Ermittlungsverfahrens • Beweissicherung • Beschlagnahme • Unterbindung der Tathandlung	• Unterlassung • Durchsuchung und Besichtigung durch Gerichtsvollzieher • Herausgabe • Auskunft • Schadenersatz • Rückruf/Vernichtung rechtsverletzender Produkte	• Außerordentliche (fristlose) Kündigung des Arbeitnehmers • Umgehende Freistellung des Arbeitnehmers • Herausgabe Arbeitsmittel / Unterlagen

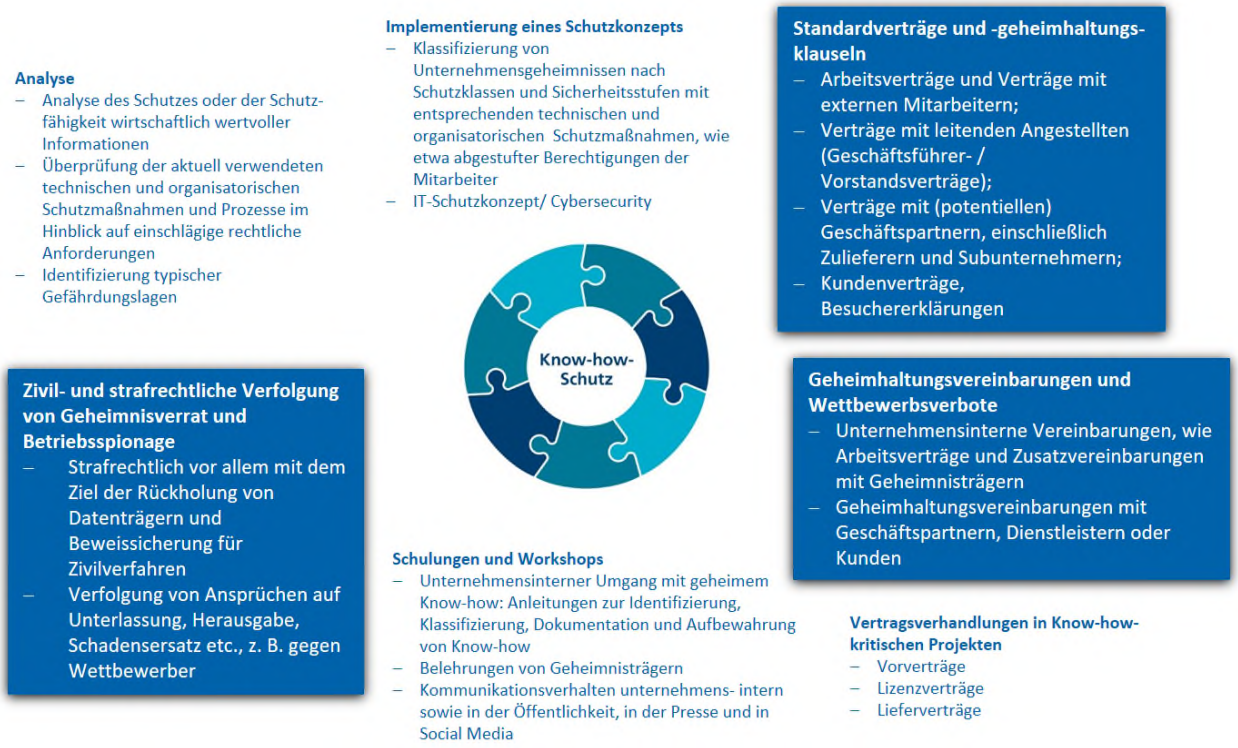
Hierbei sollte bei gleichzeitiger straf- und zivilrechtlicher Verfolgung versucht werden, mit anwaltlicher Hilfe einen „Gleichlauf" der Verfahren herzustellen: So kann es gelingen, mittels eines zivilrechtlichen Titels eine *Durchsuchung bei dem Verfahrensgegner mit derselben Maßnahme der Staatsanwaltschaft zu „koordinieren"*. Dies hat den Vorteil, dass zum einen die Gefahr, dass Beweismittel nach einem ersten „Besuch" beiseite geschafft werden, sinkt. Zum anderen erhält das geschädigte Unternehmen auf diese Weise die Chance, bei deiner Durchsuchung z.B. mit eigenen IT-Sachverständigen vor Ort zu sein, was bei einer rein behördlich veranlassten Durchsuchung in der Regel nicht möglich ist.

→ *s. hierzu auch Ziegelmayer: „Geheimnisschutz ist eine große Nische", Computer und Recht 2018, S. 693-699*

[11] LG München I (7. Zivilkammer), Beschluss vom 13.08.2019 - 7 O 3890/19; OLG Düsseldorf GRUR-RS 2019, 33225

Die Entwicklung eines Schutzkonzepts

Vor dem Hintergrund des Erfordernisses „angemessener Schutzmaßnahmen“ werden die Unternehmen auf die Richtlinie reagieren und insbesondere ihre Geheimhaltungskonzepte prüfen müssen. Ein „ganzheitliches Schutzkonzept“ umfasst im groben Überblick folgende Aspekte (s. dazu auch die → *Checkliste im Anhang*):



Ein solches Schutzkonzept lässt sich für beinahe jedes Unternehmen in Abhängigkeit von Unternehmensgröße und Umfang der Geschäftsgeheimnisse sinnvoll einrichten. Dabei geht es nicht darum, ein „weiteres Compliance-System“ zu errichten, sondern die Schutzinteressen mit anderen Bereichen abzugleichen und Maßnahmen vernünftig zu kombinieren.

Viele praktische Maßnahmen zum Geheimnisschutz überschneiden sich z.B. mit ohnehin vorhandenen Maßnahmen der allgemeinen IT-Sicherheit und des Datenschutzes. Häufig mangelt es allein daran, dass sich für dieses Thema im Unternehmen keine klare Zuständigkeit findet und deshalb einfache und naheliegende Maßnahmen ausbleiben. So können beispielsweise über Schutzrechtanmeldungen nicht schützbare Informationen gleichwohl geheim gehalten und sogar durch technische Tools „gerichtsfest“ gemacht werden. Ein Beispiel hierfür ist der Dienst „WIPO PROOF“ der Weltorganisation für Geistiges Eigentum (WIPO), der einen digitalen Fingerabdruck mit Datum und Zeitstempel jeder Datei bereitstellt und so deren Existenz zu einem bestimmten Zeitpunkt beweist[12].

Berücksichtigt man, dass Unternehmen selbst „Informationsgesellschaften“ sind, in denen Bedeutung und Wert von Informationen als Wirtschaftsgut stetig zunimmt, sind die Kosten des Abflusses von Know-how in aller Regel höher als jene für die Schutzmaßnahmen.

■

[12] https://www.wipo.int/wipoproof/en/index.html#

Anhang 1: Checkliste Know-how-Schutz im Unternehmen

Die folgende Check-Liste fasst wesentliche Eckpunkte für den Know-how-Schutz im Unternehmen entsprechend dem GeschGehG stichwortartig zusammen.

Identifikation und Bewertung von Geheimnissen und ihrer Träger

- **Festlegung eines *Informationsmanagement-Teams:***
  - zuständig für die Einrichtung eines wirksamen Know-how-Schutzes
  - angesiedelt z.B. bei Compliance-Funktion oder IP-Abteilung (besondere Sachnähe zu IP-Themen)
  - gesondertes Budget sinnvoll (besonderes Compliance Thema, ggf. Abgrenzung zu IP-Abteilung, IT, Datenschutz notwendig)
- **„Gap"-Analyse:**
  - Identifikation sensibler und für den Geschäftsbetrieb „wesentlicher" oder „geschäftskritischer" Informationen
  - Identifikation der Wissensträger (Personen, Systeme) und Bewertung der Risiken
  - Identifikation strategischer und operativer Lücken im Geheimnisschutz
- **Wirtschaftliche Bewertung von Know-how / Geschäftsgeheimnissen**
- **Risikobewertung:**
  - Bewertung des Risikos des Abflusses von Know-how durch Belegschaft, Geschäftspartner, Wettbewerber, Wirtschaftsspionage, staatliche Spionage
  - Aufstellung eines spezifischen Maßnahmenplans („Risk Mitigation Plan"), ggf. als Bestandteil des allgemeinen Risikomanagements

Richtlinien, Prozesse, Dokumentation und Schulung

- **Interne Richtlinien, Richtlinie für Geschäftspartner:** Ausarbeitung unternehmensweiter Richtlinien zum Schutz von Betriebs- und Geschäftsgeheimnissen gegenüber Belegschaft und externer Vertragspartner (z.B. innerhalb der Lieferkette)
- **Einführung von Standardprozessen zum Schutz von Geheimnissen:** Ausarbeitung von Prozessen zum Umgang mit sensitiven Informationen des Unternehmens in verschiedenen Bereichen, insbesondere
  - Recruiting und Exit Management (z.B. „Exit-Gespräche" mit Arbeitnehmern und zeitgebundene Rückgabeverpflichtungen bei Wissensträgern)
  - Speicherung und Aufbewahrung geheimer Informationen, Umgang mit Dokumenten und Datenträgern (z.B. Geheimhaltungsrichtlinie)
  - Nutzung externer Ressourcen und Kommunikation (Cloud-Dienste, Social Media etc.)
- **Vorgaben zur Kennzeichnung und Absonderung von Geheimnissen:** Implementierung eines abgestuften Konzepts zur Kennzeichnung und Bewertung von Informationen als Geschäftsgeheimnisse, den Regeln für den Zugang sowie dem Umgang mit ihnen
- **Erstellung eines „Inventars" oder einer „Trade Secret Registry":** Dokumentation aller schützenswerten Geheimnisse und geheimnisrelevanten Vorgänge, insbesondere mit Angaben zur Nutzung und möglicher Herausgabe dieser Informationen aus der Sphäre des Unternehmens
- **Schulung der Mitarbeiter, ggf. auch Externe:** „Awareness" unverzichtbar und notwendig zur wirksamen Implementierung von internen Richtlinien

Sicherheit

- **Physische Sicherheit / IT-Sicherheit**
  - Know-how-Schutz ist nicht nur IT-Sicherheit, aber beinhaltet auch IT-Sicherheit (Gleichlauf mit anderen Schutzbereichen, IT-Sicherheit allgemein, Datenschutz)
  - Physischen und IT-Sicherheitssysteme sind auf das Ziel des Schutzes vertraulicher Informationen auszurichten
- **Implementierung des „Need to know"-Prinzips**: Zugang zu sensiblen Informationen erhalten nur Personen, Abteilungen oder Gruppen, die es angeht
- **Unternehmens- und Werksschutz:** Sicherheitspersonal, ID-Karten, zulässige Überwachungsmaßnahmen
- **Clean Desk/Clean-Desktop:** Es ist sicherzustellen, dass vertrauliche Informationen nicht unbeaufsichtigt herumliegen oder z.B. auf Whiteboards oder in Papierkörben verbleiben

- **IT/Cybersicherheit**: Sicherer Serverstandort, Passwortmanagement- und richtlinien, Beschränkungen für externe Datenträger, Beschränkungen für Drucken und Screenshots, Firewalls, Verschlüsselungsmechanismen, Tracking von auffälligen Downloadaktivitäten
- **Abschluss einer geeigneten Cyberversicherung**

Vertragsgestaltung

- **Vertraglicher Geheimnisschutz:**
  - Geheimhaltungsklauseln mit Lieferanten, Kooperationspartnern, Kunden und sonstigen Geschäftspartnern
  - Identifikation von potenziellen Schwachstellen bei Schutz und Management von Geheimnissen durch Geschäftspartner
- **Nutzung von Standard-Geheimhaltungsklauseln:** Kein Austausch von Geheimnissen ohne vertragliche Geheimhaltungspflicht insbesondere
  - in der Produktentwicklung
  - in (Arbeits-)verträgen mit internen und externen (festen/freien) Mitarbeitern, Dienstleistern
  - in Verträgen mit leitenden Angestellten (Geschäftsführer-/Vorstandsverträge)
  - in Verträgen mit (potenziellen) Geschäftspartnern, einschließlich Zulieferer und Subunternehmer
  - in relevanten Kundenverträgen
  - bei Unternehmensbesuchern mit Zugang zu sensiblen Bereichen
- **Nutzung detaillierter Vertraulichkeitsvereinbarungen („NDA“) in Know-how kritischen Projekten/Verträgen:** individuelle und konkrete Geheimnisschutzklauseln zum Schutz von Know-how, in denen die Geheimisse konkret identifiziert sind, im Einzelfall mit Vertragsstrafe abgesichert (z.B. bei Entwicklungsverträgen, Kooperationsverträgen, Lizenzvereinbarungen, M&A-Transaktionen)

Rechtsdurchsetzung, Notfallplan

- **Festlegung eines Einsatzteams für den aktuellen Fall von (drohendem) Know-how-Verlust** mit Definition der internen Berichtsketten und Zeitfenster („Rapid Response“) sowie möglicher Einsatz externer Berater/Forensiker/Anwälte
- **Während Beweisermittlung/Recovery:**
  - Geräte und Datenträger nie selbst untersuchen/auswerten: Aufgabe (externer) IT Forensik
  - Strengste Geheimhaltung bei der internen Untersuchung
  - Fristen beachten: Strafantrag 3 Monate, Einstweilige Verfügung max. 1 Monat nach Kenntnis!
  - Sorgfältige Abwägung vor Anhörung des Betroffenen, weil Beweise unterdrückt werden können
  - In der Regel keine vorgehende Abmahnung, sondern unmittelbar gerichtlicher Rechtsschutz
- **Abwägung straf- und zivilrechtlicher Folgen**
  - Gefahren für das Unternehmen?
  - Gerichtsbarkeit: Unwägbarkeiten bei Zuständigkeit der Arbeitsgerichte
  - Im Falle der Ausschöpfung aller rechtlichen Möglichkeiten: Koordination von zivil- und strafrechtlichen Vorgehen (etwa bei Durchsuchungen und Beweisverwertung)

Anhang 2: Klauselbeispiele

Arbeitsvertragliche Verschwiegenheitsverpflichtung/Rückgabeverpflichtung:

> *„XY verpflichtet sich gegenüber der . . . . . auch nach Beendigung des Beschäftigungsverhältnisses für eine Dauer von . . . . . zu strenger Geheimhaltung der ihm während der Dauer des Beschäftigungsverhältnisses bekannt gewordenen Interna und vertraulichen Angelegenheiten, insbesondere in Bezug auf das spezielle Herstellungsverfahren des . . . . . "*

> *„XY verpflichtet sich, über Geschäfts- und Betriebsgeheimnisse und alle vertraulichen Informationen, die ihm im Rahmen seiner Tätigkeit bei . . . . . zur Kenntnis gelangen, auch nach Beendigung des Arbeitsverhältnisses Stillschweigen zu bewahren. Vertrauliche Informationen sind alle geschäftlichen, betrieblichen oder sachlichen Informationen, die von einem Vorgesetzten oder XY selbst ausdrücklich als vertraulich bezeichnet werden oder deren Geheimhaltungspflicht für XY erkennbar ist. Im Zweifelsfall hat XY eine Weisung eines Vorgesetzten zur Vertraulichkeit bestimmter Tatsachen einzuholen.*
>
> *Die betrieblichen Sicherheitsbestimmungen, insbesondere die Know-how-Schutz-Richtlinie sind zu beachten. Vertrauliche Dokumente und geheim zu haltende Schriftstücke wie Zeichnungen, Modelle . . . . . sind unter Verschluss zu halten."*

> *„Geschäftliche und betriebliche Unterlagen aller Art, gleichgültig ob im Original, in elektronischer Form, im Durchschlag, in Vervielfältigung oder im Entwurf einschließlich persönlicher Aufzeichnungen über dienstliche Angelegenheiten, sind als von . . . . . anvertrautes Eigentum zu betrachten und auf Verlangen jederzeit, spätestens aber bei Beendigung des Arbeitsverhältnisses unverzüglich an . . . . . herauszugeben. Zurückbehaltungsrechte sind ausgeschlossen."*

Freistellung:

> *„. . . . . ist berechtigt, XY während der Kündigungsfrist jederzeit unter Fortzahlung des Gehaltes von der Arbeitsleistung freizustellen. Die Freistellung erfolgt unwiderruflich unter Anrechnung sämtlicher bestehender oder erst noch entstehender Urlaubs- oder Freizeitausgleichansprüche."* (Hieran anschließend ggf. Vereinbarung bzgl. Anwendung des § 615 S. 2 BGB.)

Wettbewerbsverbote können mit Verschwiegenheitsverpflichtungen gekoppelt werden. Beispiel:

> *„XY verpflichtet sich, für die Dauer von zwei Jahren nach Beendigung des Arbeitsverhältnisses, nicht selbstständig oder unselbstständig für ein Unternehmen tätig zu werden, das mit dem Arbeitgeber in Wettbewerb steht. Das Wettbewerbsverbot gilt räumlich für [Gebietsbeschreibung] und für alle Gebiete, in denen die Gesellschaft bei Beendigung des Arbeitsverhältnisses tätig ist."*

Reverse Engineering

Nachdem die Richtlinie Reverse Engineering für zulässig erklärt, kann ein „Mindestschutz" (nur) gegenüber dem Vertragspartner z.B. mit folgender Klausel erzielt werden:

> *„Die empfangende Partei verpflichtet sich, keine Materialien zu eigenen geschäftlichen Zwecken direkt oder indirekt rückzuerschließen („Reverse Engineering") oder dies zu versuchen, sofern nichts anderes schriftlich vereinbart ist. Insbesondere darf die empfangende Partei die in den Materialien enthaltenen [Elemente, Materialien, Zutaten, Komponenten, Formeln, Verfahren, Quellcode] nicht dekompilieren, analysieren, disassemblieren oder auf andere Weise versuchen, diese rückzuentwickeln oder zu erschließen."*

→ In geeigneten Fällen sollte die Aufnahme von Vertragsstrafenvereinbarungen erwogen werden

■

Anhang 3: Interne Richtlinie zum Geheimnisschutz

Das folgende Beispiel beinhaltet Eckpunkte für den Geheimnisschutz im Unternehmen. Eine Richtlinie muss sich im Einzelfall an den besonderen Gegebenheiten des Unternehmens orientieren und zum sonstigen Bestand interner Richtlinien passen. Es handelt sich daher nicht um ein Muster, sondern lediglich um ein Beispiel.

Richtlinie zum Geheimnisschutz im Unternehmen ABC

1. Anwendungsbereich

Diese Richtlinie regelt den Umgang mit vertraulichen Informationen („Know-how“) innerhalb unseres Unternehmens. Sie gilt für [*die gesamte Unternehmensgruppe/bestimmte Unternehmen/Abteilungen*].

2. Ziele des Know-how-Schutzes

Der Schutz unseres Know-hows ist ein wesentlicher Bestandteil unserer Unternehmenskultur und Voraussetzung für den Unternehmenserfolg. Es ist wichtig, dass Sie sich in Bezug auf sensible Informationen der Notwendigkeit eines angemessenen Geheimnisschutzes bewusst sind.

Wir erwarten daher, dass Sie

- unser eigenes Know-how jederzeit schützen,
- die Vertraulichkeit von Informationen in Bezug auf unsere Geschäftspartner und Kunden wahren;
- in der Lage sind, Risiken für den Schutz vertraulicher Situationen zu erkennen, durch geeignete Maßnahmen zu vermeiden bzw. zu mindern und verbleibenden Risiken entschlossen begegnen.

3. Organisation des Know-how-Schutzes im Unternehmen

Die Geschäftsführung hat zur Umsetzung der Sicherheitsziele ein „Know-how-Schutz-Team“ [Alt. *Stabsstelle/Abteilung*] eingerichtet und diesem die Aufgabe übertragen, einheitliche Vorgaben für den Sicherheitsprozess zu erstellen, für die ausreichende Sensibilisierung aller Mitarbeiter/innen zu sorgen sowie die Einhaltung aller damit zusammenhängenden Richtlinien angemessen zu überprüfen bzw. überprüfen zu lassen.

Nach dieser Richtlinie ist zunächst jede Organisationseinheit unseres Unternehmens für die Sicherheit der eigenen Daten und deren Verarbeitung verantwortlich. Im Rahmen dieser Verantwortung wird jede Organisationseinheit eine Aufstellung ihrer Assets (Daten, Systeme und Prozesse) anfertigen, eine Risikoanalyse und -bewertung nach vorgegebenem einheitlichen Muster dafür durchführen und in regelmäßigen Abständen sowie nach erheblichen Änderungen aktualisieren. Dort wo eine Klassifizierung von Informationen erforderlich ist, wird der Umgang mit solchen Informationen in einer separaten Richtlinie geregelt.

[*Weitere Angaben zu Organisation, Zuständigkeiten etc*.]

4. Anforderungen an Mitarbeiter

Das Vertrauen unserer Kunden und Geschäftspartner ist eine der Grundlagen für unser Geschäft. Um für den Schutz unseres Know-how gerüstet zu sein,

- erhalten Sie bei Bedarf für den jeweiligen Arbeitsplatz spezielle Sicherheitsregeln, die insbesondere eine Meldepflicht bei Sicherheitsvorkommnissen in Bezug auf unser Know-how beinhalten;
- sind Sie verpflichtet, regelmäßig an den angebotenen Schulungen zum Know-how-Schutz teilzunehmen.

Im Haus

…erreichen wir unser Ziel durch die Einhaltung folgender Regeln:

- Sie selbst entscheiden mit darüber, ob es sich bei Informationen, mit denen Sie im Rahmen Ihrer Tätigkeit in Berührung kommen, um unser schützenswertes Know-how handelt. Wenn Sie erkennen, dass Informationen (z.B. über unsere Preise, Kundenlisten oder die Strategien von Unternehmen für den Vertrieb) sensibel sind, sorgen Sie für eine entsprechende Kennzeichnung (z.B. durch Sichtvermerke, Kennzeichnung von E-Mails als „vertraulich“).
- Der Missbrauch oder die Offenlegung von Informationen, die als vertraulich oder geschützt angesehen werden oder entsprechend gekennzeichnet sind, ist sowohl während als auch nach Ihrer Beschäftigung bei [*Unternehmen*] verboten und stellt eine Verletzung Ihres Arbeitsvertrags dar. Eine solche Offenlegung kann außerdem schwerwie-

gende Nachteile für unser Unternehmen und Sie zur Folge haben. Alle vertraulichen oder geschützten Informationen, die Sie besitzen oder auf die Sie Zugriff haben sowie die zugehörigen Dokumente in materieller oder elektronischer Form sind Eigentum von [*Unternehmen*]. Dabei spielt es keine Rolle, wo sich die Informationen befinden.

- Alle entsprechenden Informationen müssen am Ende Ihres Beschäftigungsverhältnisses an [*Unternehmen/HR*] zurückgegeben werden. Jede Entnahme, jeder Download und jede andere untersagte Verwendung oder Offenlegung derartiger Informationen kann als Verletzung von Geschäftsgeheimnissen angesehen und in letzter Konsequenz auch strafrechtlich verfolgt werden.
- Zudem sollten Sie Schritte unternehmen, um eine versehentliche Offenlegung vertraulicher oder geschützter Informationen zu verhindern. Sprechen Sie mit Außenstehenden, auch mit Familie und Freunden, nicht über nichtöffentliche oder vertrauliche Informationen von [*Unternehmen*]. Besprechen Sie diese Informationen auch nicht hörbar an öffentlichen Orten (wie z.B. Restaurants, Bahnabteil). Selbst innerhalb von [*Unternehmen*] sollten Sie vertrauliche Informationen nur dann mit anderen teilen, wenn dies sachlich notwendig ist und in die Zuständigkeit der betreffenden Personen fällt.
- Ergreifen Sie außerhalb der [Unternehmen-]Standorte besondere Vorsichtsmaßnahmen zum Schutz der Informationen, sowohl in gedruckter als auch in elektronischer Form, um eine versehentliche Offenlegung, z.B. an öffentlichen Orten, zu vermeiden.

Im Wettbewerb

…. ist zu erwarten, dass Sie z.B. auf Veranstaltungen oder in Meetings auf Personen treffen werden, die für Wettbewerber, Partner, Lieferanten oder Kunden von [*Unternehmen*] arbeiten. Seien Sie im Umgang mit diesen Personen vorsichtig mit Ihren Aussagen, auch wenn die Gespräche harmlos erscheinen. Besprechen Sie mit diesen Personen keine Themen, die unser Know-how betreffen. Informieren Sie Ihren Vorgesetzten oder [*die Rechtsabteilung*] über derartige Vorkommnisse.

- Sie dürfen alle öffentlich zugänglichen Informationen über Mitbewerber von [*Unternehmen*] oder andere Unternehmen nutzen. Es ist Ihnen jedoch untersagt, sich widerrechtlich Zugang zu Geschäftsgeheimnissen oder anderen vertraulichen Informationen Dritter zu verschaffen oder diese zu missbrauchen. Unser Unternehmen verbietet daher den Einsatz unlauterer Mittel zur Beschaffung vertraulicher Informationen Dritter. Unlautere Mittel sind beispielsweise die Zahlung von Geldbeträgen, das Anbieten von Gefälligkeiten und das Anwerben von Mitarbeitern eines Mitbewerbers von [*Unternehmen*] mit dem Ziel, vertrauliche Informationen Dritter zu erlangen.
- Auch wenn Sie auf rechtmäßigem Wege Informationen über ein anderes Unternehmen erlangen, sind Sie verpflichtet, die Vertraulichkeit und die zulässigen Einsatzmöglichkeiten dieser Informationen für unser Unternehmen zu überprüfen. Achten Sie beispielsweise auf Beschriftungen, die Dokumente als vertraulich kennzeichnen. Bevor Sie bewusst vertrauliche Informationen entgegennehmen, sollten Sie die Bedingungen für die Nutzung dieser Informationen festlegen.
- Unter Umständen ist im Umgang mit Geschäftspartnern eine Vertraulichkeitsvereinbarung („Non-Disclosure Agreement“ – NDA) erforderlich, die die Nutzung, Offenlegung und Weitergabe der Informationen einschränkt. Wenn Sie vertrauliche Informationen auf rechtmäßigem Weg erhalten haben und eine Vertraulichkeitsvereinbarung dafür vorliegt, dürfen Sie die Informationen nur entsprechend dieser Vereinbarung nutzen, vervielfältigen, offenlegen oder weitergeben.
- Sie müssen sich außerdem an rechtliche Verpflichtungen gegenüber Ihren früheren Arbeitgebern halten. Diese können beispielsweise die Nutzung und Offenlegung vertraulicher Informationen, die Anwerbung früherer Kollegen für die Arbeit bei [*Unternehmen*] oder Wettbewerbsverbote betreffen. Wenden Sie sich bei Fragen zu diesen Verpflichtungen an [*die Rechtsabteilung*].
- Veröffentlichen Sie ohne ausdrückliche vorherige Genehmigung keine Informationen über [*Unternehmen*] in Social Media wie Blogs oder sozialen Netzwerken.

Sollten Sie eine der im Folgenden aufgeführten Anfragen erhalten, antworten Sie ausschließlich mit einem Verweis an die entsprechenden Kontakte:

Presseanfragen	Abteilung: …	Ansprechpartner: …
Analysten oder Investoren	Abteilung: …	Ansprechpartner: …
Behörden	Abteilung: …	Ansprechpartner: …
Forschungseinrichtungen	Abteilung: …	Ansprechpartner: …

Diese Richtlinie tritt am [Datum] in Kraft.