



Vom unzulässigen Download zur Industriespionage „Secrecy-Governance“ die Überlebensstrategie für Unternehmen

„Secrecy-Governance“ ist der ganzheitliche Schutz von Betriebs- und Geschäftsgeheimnissen und ein Beitrag zur Einhaltung der Unternehmens-Compliance. Unternehmerische Geheimnisse sind häufig die entscheidende Existenzgrundlage eines Unternehmens. Dies gilt sowohl für Geschäftsgeheimnisse wie Kundenlisten als auch für Betriebsgeheimnisse wie beispielsweise technische Geheimnisse. Werden sie durch einen Unbefugten, gar einen Konkurrenten verwertet, kann dies zu erheblichen wettbewerblichen Nachteilen bis hin zur Unternehmensvernichtung führen.

Seitens der Gesetzgebung sind Unternehmen zur Einhaltung von Gesetzen wie Bundesdatenschutzgesetz (BDSG), Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und natürlich Vertragsrecht verpflichtet. Sie haben im Wesen gemeinsam, den Schaden von Unternehmen abzuwenden und in besonders gefährdeten Bereichen ein Frühwarnsystem einzuführen. Dieses gilt nicht nur für börsenorientierte Unternehmen, die dem KonTraG bzw. Sarbanes-Oxley-Act (SOX) verpflichtet sind, um die IT revisionssicher aufzustellen und dafür ein Risikomanagement einzuführen.

Die Einhaltung dieser Gesetze erhöht zwar das Schutzniveau der Firmendaten, bietet den Unternehmen aber eine unzureichende rechtliche Handhabe bei Missbrauch von Betriebs- und Geschäftsgeheimnissen.

Schwacher gesetzlicher Schutz

Von Gesetzes wegen - also ohne eine gesonderte Vereinbarung - sind Unternehmensgeheimnisse, obwohl sie ein immaterielles Wirtschaftsgut von erheblicher Bedeutung darstellen, nur unzureichend geschützt. Zwar enthalten §§ 17 bis 19 UWG wenig griffige Straftatbestände, deren Verletzung auch zivilrechtliche Unterlassungsansprüche und Schadensersatzansprüche begründet (§§ 3, 4 Nr. 10, 11 UWG i.V.m. §§ 8,9 UWG sowie §§ 1004 bzw. 823 Abs. 2 BGB). Allerdings schützen die §§ 17 - 19 UWG nach ständiger Rechtsprechung nicht davor, dass ein ausgeschiedener Mitarbeiter ihm während seines Arbeitsverhältnisses anvertraute Informationen nach dessen Beendigung verwertet, solange er sie lediglich „in seinem Gedächtnis bewahrt hat“ und nicht schriftlich fixiert oder in sonstiger Weise gespeichert hat. Gleiches gilt für außenstehende Personen - etwa Zulieferer -, die im Rahmen einer wie auch immer gearteten Zusammenarbeit bestimmte Geheimnisse auf lautere Weise erfahren haben.

Vertragsrecht als Schutzwall

Für den Unternehmer ist die Kenntnis wichtiger juristischer Schutzinstrumente und der mit ihnen verbundenen Probleme entscheidend. Dies betrifft speziell das Vertragsrecht. Dabei ist zu unterscheiden zwischen Verträgen, die das jeweilige Unternehmen mit seinen Arbeitnehmer abschließt und solchen Verträgen, die es mit anderen Unternehmen - etwa Lieferanten oder Vertriebspartnern - abschließt.

Ein wichtiges Schutzinstrument sind zunächst Geheimhaltungsverpflichtungen respektive Vertraulichkeitsvereinbarungen. Sofern solche mit Arbeitnehmer abgeschlossen werden, ist zu beachten, dass sie hinreichend eingeschränkt sein müssen. Eine umfassende, über das Ende des Arbeitsverhältnisses hinausgehende Geheimhaltungsverpflichtung ist nämlich in der Sache als nachvertragliches Wettbewerbsverbot zu bewerten. Ein solches ist nur unter den engen Voraussetzungen der §§ 74 ff. HGB wirksam. Insbesondere müssen folglich eine Karenzentschädigung vereinbart und eine Höchstdauer von zwei Jahren beachtet

werden. Bei der Abfassung von Geheimhaltungsverpflichtungen mit Arbeitnehmern sollte man sich also am Grundsatz „weniger ist mehr“ orientieren. Dies gilt letztlich auch bei Geheimhaltungsvereinbarungen zwischen Unternehmen: Hier ist nämlich im Einzelfall aus kartellrechtlichen Gründen eine genaue Identifizierung des geheimen Know-hows und mithin eine Eingrenzung des Schutzbereichs erforderlich (vgl. Art. 1 Ziff. 3 VO(EG) Nr. 772/2004). Schließlich muss offenkundig gewordenes Wissen stets von einer Geheimhaltungsverpflichtung ausgenommen sein.

Innerbetriebliche Geheimhaltungsvereinbarungen sollten unbedingt flankiert werden von einer Verpflichtung auf das Datengeheimnis gem. § 5 BDSG. Hierdurch werden die Mitarbeiter von Anfang an zu sensiblem Umgang mit personenbezogenen Daten, insbesondere Kundendaten - solche stellen regelmäßig wesentliche Geschäftsgeheimnisse dar -, angehalten. In entsprechenden Datenschutzvereinbarungen kann einem Arbeitnehmer ein Überschreiten der ihm eingeräumten Datenverarbeitungsberechtigung sowie die Umgehung technischer Schutzmechanismen, auf die noch eingegangen wird, untersagt werden. Auf diese Weise kann das oft als lästig empfundene BDSG einen effektiven Beitrag zum Schutz von Geschäftsgeheimnissen leisten.

Nachvertragliche Wettbewerbsverbote können zur Falle werden

Geheimhaltungsverpflichtungen und Datenschutzverpflichtungen bieten letztlich nur einen begrenzten, „löcherigen“ Schutz. Daher stellt sich im Einzelfall stets die Frage, ob nicht zusätzlich auch vertragliche und nachvertragliche Wettbewerbsverbote vereinbart werden sollten. Dies bedarf einer eingehenden Nutzen-Risikoanalyse. Nachvertragliche Wettbewerbsverbote mit Arbeitnehmern unterliegen den Schranken der §§ 74 ff. HGB: Es ist also die Schriftform zu wahren. Ferner muss die unterzeichnete Vereinbarung dem Arbeitnehmer ausgehändigt werden. Außerdem gilt der Grundsatz der bezahlten Karenz, d.h. die Vereinbarung muss vorsehen, dass der Arbeitnehmer für jedes Jahr des nachvertraglichen Wettbewerbsverbotes wenigstens die Hälfte der von ihm zuletzt bezogenen vertraglichen Leistung erhält.

Zu beachten ist auch, dass nachvertragliche Wettbewerbsverbote längstens für eine Dauer von zwei Jahren abgeschlossen werden dürfen.

Nachvertragliche Wettbewerbsverbote enthalten Wettbewerbsbeschränkungen. Werden sie zwischen Unternehmen vereinbart, sind daher kartellrechtliche Schranken zu beachten (vgl. hierzu § 1 GWB, Art. 81 Abs. 1, 3 EGV i.V.m. Art. 5 VO (EG) 2790/1999). Im Grundsatz ist hier von der so genannten Immanenztheorie auszugehen. Dieser zufolge sind Wettbewerbsverbote kartellrechtlich zulässig, soweit sie der Absicherung des Zwecks des Hauptvertrages dienen. Es bedarf insoweit also einer sorgfältigen Interessenabwägung unter Beachtung des bereits angesprochenen Grundsatzes „weniger kann mehr sein“. Dies gilt umso mehr, als bei jedem Wettbewerbsverbot zu prüfen ist, ob es nicht wegen Verstoßes gegen § 138 BGB, also das Verbot sittenwidriger Vereinbarungen, nichtig ist. Dabei ist die Bedeutung des Grundrechts der Berufsfreiheit (Art. 12 GG) mit zu berücksichtigen. Ein nachvertragliches Wettbewerbsverbot zwischen Unternehmen soll deshalb nur dann wirksam sein, wenn es aufgrund schutzwürdiger Interessen gerechtfertigt sowie sachlich, örtlich und zeitlich begrenzt ist.

Auch im Bereich der Wettbewerbsverbote gilt also, dass man sich auf entsprechende Vereinbarungen nur dann „einigermaßen“ verlassen kann, wenn sie von erfahrenen Beratern sorgfältig, unter Berücksichtigung sämtlicher Besonderheiten des Einzelfalls formuliert worden sind. Bedient man sich einer solchen Hilfe, wird man durchaus ein angemessenes Schutzniveau erreichen können, wobei man sich stets klarmachen sollte, dass ein vollkommen lückenloser Schutz wohl niemals zu erreichen ist.

Flankieren sollte man Geheimhaltungsverpflichtungen bzw. nachvertragliche Wettbewerbsverbote zudem unbedingt durch vertragliche Regelungen, durch die man sich die Rechte an den Arbeitsergebnissen des jeweiligen Arbeitnehmers bzw. Kooperationspartners einräumen lässt. Auch hier sind natürlich die durch zwingende gesetzliche Regelungen gesteckten Grenzen insbesondere des Arbeitnehmererfinderrechts zu beachten.

Sicherungsmaßnahmen technischer und organisatorischer Art

So notwendig die vorstehend angesprochenen juristischen Sicherungsmaßnahmen auch sind: Mindestens ebenso wichtig sind technische und organisatorische Sicherungsmaßnahmen, die einer unbefugten Geheimniserlangung und -verwertung entgegenwirken. Diese sollten ggfs. in innerbetrieblichen IT-Sicherheitsrichtlinien näher konkretisiert werden.

Als Beispiele für entsprechende technische und organisatorische Maßnahmen sind die durch das BDSG in Anlage zu § 9 Satz 1 geforderten Maßnahmen zu nennen. Jedes Unternehmen egal welcher Gesellschaftsform und Größe ist dem BDSG verpflichtet, hat entsprechende Verfahrensverzeichnisse vorzuhalten und kann damit bereits das vorhandene Datenschutzniveau analysieren bzw. verbessern. Unter gewissen Umständen bietet sich auch die Einführung eines IT-Risiko-Managementsystem, z.B. nach ISO 27001, an.

Auch die Verschlüsselung von E-Mails und, natürlich nur im arbeitsrechtlich zulässigem Umfang, die Überwachung von Mitarbeitern z.B. durch Registrieren aller ein- und ausgehenden E-Mails sollten betrachtet werden. Darüber hinaus sollte man sich über den Umfang der Nutzung von „Home-Offices“ Gedanken machen. Da diese Home-Offices meist nur einer schwachen Security-Policy unterliegen und unzureichend auf Veränderungen überwacht werden, gibt es äußerst hoch einzustufende Risiken. Nur drei gravierende Beispiele: Die Konkurrenz bekommt einen Einblick in Know-how oder Kundendaten. Ein Notebook wird gestohlen und die auf der Festplatte gespeicherten Daten sind unverschlüsselt. Die Kundendaten werden durch eine Havarie zerstört und es gibt keine Datensicherung für eine Rekonstruktion.

Nur wenn ganzheitlich alle erforderlichen technischen sowie organisatorischen Maßnahmen umgesetzt werden, wird das Datenschutzniveau im Unternehmen erhöht. In der Praxis werden meist aus Unkenntnis nur punktuelle Maßnahmen umgesetzt, die in der Folge den Nutzen in Frage stellen. Sollte die entsprechende

Fachkunde im Unternehmen nicht vorhanden sein, ist die Inanspruchnahme von sachkundigen Stellen mehr als empfehlenswert.

„Secrecy-Governance“ ist das Geheimnis-Managementsystem

Nur ein effektives, den jeweiligen Unternehmensbesonderheiten angepasstes Zusammenspiel zwischen den vorstehend dargestellten juristischen und technischen Maßnahmen des Geheimnisschutzes vermag zu einem hinreichend befriedigenden Geheimnisschutzniveau verhelfen. In vielen Unternehmen wird es zudem sowohl aus arbeitsrechtlichen Gründen als auch aus praktischen und psychologischen Gründen nicht ohne weiteres möglich sein, von heute auf morgen von einem schwachen Geheimnisschutz zu einem strengen Geheimnisschutzregiment zu wechseln. Hier bedarf es strategischer Konzepte, wie man mittel- bis langfristig ein hinreichendes Geheimnisschutzniveau erreichen kann. Letztlich muss mit Augenmaß und Fingerspitzengefühl ein effizientes Geheimnisschutzmanagement, das technische und juristische Schutzmaßnahmen miteinander kombiniert, aufgebaut werden.

Kontakt:

Rechtsanwalt und Notar
Fachanwalt für gewerblichen Rechtsschutz Dr. H.-Christian Heyn
RAe Ohletz Willuhn Denker Heyn, Essen
Rüttenscheider Str. 120
45131 Essen
Tel. 0201 - 7248120
Homepage: <http://www.rasowd.de>

Dipl.-Ing Thomas Eckert
eckert-security Management, Heiligenhaus
Erich-Ollenhauer-Str. 60
42579 Heiligenhaus
Tel. 02056 - 57140
Homepage: <http://www.drqm.de>

Disclaimer

Die Übernahme von Inhalten in Datenbestände, die ausschließlich für den privaten Gebrauch eines Nutzers bestimmt sind wird zugestimmt. Die Übernahme und Nutzung der Daten, auch Auszugweise, zu anderen, insbesondere kommerziellen Zwecken, bedarf der schriftlichen Zustimmung der Autoren.