

9. ZAAR-Kongress:
„Know-How-Schutz im Arbeitsrecht“

Freitag, 5. Mai 2012



Know-How und Geschäftsgeheimnisse sind begehrte Assets eines Unternehmens. Ihr Schutz sollte daher einen zentralen Platz im General Management jedes Unternehmens einnehmen. Dennoch ist der Know-How-Schutz in vielen Unternehmen nur sehr schwach ausgeprägt. Auch Wissenschaft und Rechtsprechung haben sich bisher nur in geringem Umfang mit diesem Thema beschäftigt. Der Know-How-Schutz stand daher im Mittelpunkt des 9. ZAAR-Kongresses am 4. Mai 2012 im Paulaner am Nockherberg in München.

I. Know-How-Schutz als Managementaufgabe



Der 9. ZAAR-Kongress wurde durch den Vortrag von Herrn Professor Dr. Christoph Ann eröffnet. Zur Definition des Begriffes „Know-How“ zog Professor Ann Art. 39 TRIPS heran. Danach sind Merkmale von Know-How seine Nicht-Offenkundigkeit, die aktive Geheimhaltung, seine Geheimschutzfähigkeit sowie der wirtschaftliche Wert, der aufgrund des Geheimnischarakters entsteht. Der Referent bezeichnete den Know-How-Schutz als eine Strategieentscheidung. Geheimnisschutz muss kosteneffizient und strategisch einsetzbar sein. Besonderen Wert

wurde dabei auf den Umstand gelegt, dass der Know-How-Schutz eine Frage des General Managements sein sollte. Es muss klar entschieden werden, was wovon geschützt werden soll und ob dieser Schutz durch Patentanmeldung oder Geheimhaltung stattfinden soll. Für den Know-How-Schutz sollte sich das Unternehmen gerade dann entscheiden, wenn es um die sogenannten „Kronjuwelen“ des Unternehmens geht. Der Know-How-Schutz betrifft mehrere Abteilungen im Unternehmen. Während die Patentabteilung über das Schutzregime (Patent oder Geheimhaltung) entscheidet, ist die Rechtsabteilung für den vertraglichen Know-How-Schutz verantwortlich, der Werkschutz für den Objektschutz und die IT-Abteilung für den IT-Schutz. Laut dem Sicherheitsforum BaWü sind 70 % aller Täter Angestellte

des Unternehmens. Gründe hierfür sind die fehlende Sensibilität, die steigende Fluktuation sowie die sinkende Loyalität. Know-How-Schutz ist daher auch eine Frage des Informationsschutzmanagements. Das Bewusstsein der Mitarbeiter für den Geheimnisschutz muss geschärft werden. Es müssen klare Regeln aufgestellt, Zugangsregelungen erlassen und Arbeitsverträge angepasst werden. In der anschließenden Diskussion wurden vor allem Fragen zur Haftungskonsequenz nach § 91 AktG erläutert.

II. Spionage, Sicherheit und Compliance in der Praxis



Als zweiter Redner referierte Herr Rainer Benne (selbständiger Unternehmensberater / CFS Consult) über das Thema „Spionage, Sicherheit und Compliance in der Praxis“. Zu Beginn stellte der Referent die Risikofaktoren für Unternehmenskriminalität und Informationsfluss dar. Hierzu gehören zum Beispiel Gier, Sucht, mangelndes Selbstbewusstsein, Statusangebote, Wertschätzungsangebote, Rache, Rivalität, Manipulation und Profilierungssucht. Der Informationsfluss erfolgt dabei weitgehend über die klassische technische Spionage. Dem kann durch

das „Härten“ der Systeme sowie geeignete Sicherheitskonzepte entgegengewirkt werden. Gefestigte Systeme werden grundsätzlich weniger angegriffen als ungefestigte, da mit gefestigten Systemen ein höherer Zeitwert und ein höheres Entdeckungsrisiko einhergehen. Im zweiten Teil der Präsentation stellte Herr Benne die Neutralisationstechniken von Sykes und Matza dar. Danach rechtfertigten Menschen ihre kriminellen Handlungen durch das Leugnen der Verantwortung (Leugnen der Willentlichkeit, Folgenminimierung und sozialer Vergleich mit anderen), durch die Verneinung des Schadens sowie durch Ablehnung des Opfers. Anschließend ging der Referent auf die Prävention von Geheimnisverrat ein. Durch den Faktor Mensch entsteht eine Schnittstelle zwischen Sicherheits-, Compliance- und Personalmanagement. Der Mensch ist nicht nur Risiko-, sondern auch Chancenträger. Offenheit, Ehrlichkeit und Loyalität müssen erlernt und kulturell verankert werden. Es ist die Aufgabe des Arbeitgebers diskretions- und loyalitätsnegierende Faktoren zu erkennen und zu beheben. Besonders hervorgehoben wurde die Mitarbeiterzufriedenheit nach dem Integrationsansatz. Der Integrationsansatz beruht auf dem Punkt der intrinsischen Motivation der Mitarbeiter zu einer positiven Einstellung gegenüber den ethischen Prinzipien der Unternehmensführung. Der Referent empfiehlt daher die Schaffung einer Wertekultur sowie eines ökonomischen Systems, das von Compliance getragen wird.

III. Arbeitsrechtliche Vorsorgekonzepte gegen Industriespionage und Geheimnisverrat



Nach der Mittagspause ging es weiter mit dem Vortrag von Herrn Rechtsanwalt Dr. Martin Brock (Loschelder Rechtsanwälte, Köln) zum Thema „Arbeitsrechtliche Vorsorgekonzepte gegen Industriespionage und Geheimnisverrat“. Geschäftsgeheimnisse sind Tatsachen im Zusammenhang mit dem Geschäftsbetrieb, die nur einem engen, geschlossenen Personenkreis bekannt, also nicht offenkundig sind und bei denen zumindest ein konkludenter Gemeinhaltungswille des Betriebsinhabers sowie ein rechtliches oder wirtschaftliches Interesse an

der Gemeinhaltung besteht. Der Inhalt von Geschäftsgeheimnissen können technisches Wissen, Vertriebswissen, wirtschaftliche Daten oder auch Daten aus dem Personalbereich sein. Der gesetzliche Schutz von Geschäftsgeheimnissen während des bestehenden Arbeitsverhältnisses ergibt sich aus der Verschwiegenheitspflicht (vertragliche Nebenpflicht) sowie dem allgemeinen Verbot der Konkurrenztä-

tigkeit (§ 60 HGB). Weiterhin ist der Geheimnisschutz in §§ 17, 18 UWG, § 24 Abs. 2, 5, 18 ArbNErfG und § 5 BDSG enthalten. Nachteile der vertraglichen Verschwiegenheitspflicht sind der Umstand, dass es eben nur eine vertragliche Pflicht ist, der Schadensersatzanspruch sich nur gegen den Arbeitnehmer richten kann und die Erbringung des Beweises für einen Schaden sich in der Regel als schwierig erweisen dürfte. Zu den Grenzen des vertraglichen Wettbewerbsverbots hat sich das BAG in seinem Urteil vom 24. März 2010 – 10 AZR 66/09 geäußert. Eine vertragliche Konkretisierung des Geheimnisschutzes ist grundsätzlich wirksam, die Aufnahme von sogenannten „All-Klauseln“ in den Arbeitsvertrag dagegen nicht. Besonderen Wert legte der Referent auf den nachvertraglichen Geheimnisschutz. Herausgabebeklauseln des Arbeitgebers sind zwar im Gesetz vorhanden, besser ist aber die Aufnahme von Herausgabeklauseln in den Arbeitsvertrag. Grundsätzlich die Nutzung von verkörperten Wiedergaben durch den Arbeitnehmer nach Beendigung seines Arbeitsverhältnisses verboten, das BAG hat jedoch entschieden, dass das Erfahrungswissen, das der Arbeitnehmer im Laufe seines Berufslebens erworben hat, von ihm verwendet werden darf. Abschließend wurde auf die Karenzentschädigung bei nachvertraglichen Wettbewerbsverboten eingegangen. Bei der Vereinbarung eines nachvertraglichen Wettbewerbsverbots muss die schriftliche Originalurkunde dem Arbeitnehmer ausgehändigt werden. Der Referent wies in diesem Zusammenhang auch auf das Urteil des BAG vom 5. September 1995 – 9 AZR 718/93 und das Urteil des LAG Hamm vom 23. März 2010 – 14 SaGa 68/9 hin.

IV. Arbeitsrechtlicher Umgang mit Spionagefällen



Den Abschluss der 9. ZAAR-Konferenz bildete der Vortrag von Herrn Professor Dr. Hans Hanau der Helmut-Schmidt-Universität Hamburg. Zu Beginn ging Professor Hanau auf die Notwendigkeit des rechtlichen Schutzes von Betriebsgeheimnissen ein. Strategisches Ziel muss dabei der Ausschluss der Konkurrenz sein. Umgesetzt werden kann dieses entweder durch das Erwirken eines rechtlichen Monopols durch die Anmeldung eines gewerblichen Schutzrechts oder durch die Schaffung eines faktischen Monopols. Zivilrechtlich wird das Unternehmensgeheimnis als solches nicht geschützt. Während des Arbeitsverhältnisses gilt die Verschwiegenheitspflicht nach § 241 II BGB, deren zeitliche Dimension allerdings ungeklärt ist. Nachvertraglich greift das Wettbewerbs- und Urheberrecht. Ein selbständiger Auskunfts- und Besichtigungsanspruch ergibt sich aus § 809 BGB. Verlangt der Geheimnisträger Schadensersatz, ergeben sich Probleme hinsichtlich der Schadensberechnung (konkreter Schaden, Lizenzkosten oder Gewinnabschöpfung). Problematisch ist auch die Beweismittlung, da der Arbeitnehmerschutz, das allgemeine Persönlichkeitsrecht und der Schutz der informationellen Selbstbestimmung arbeitsrechtliche Hürden bereiten. In strafrechtlicher Hinsicht wird das Betriebsgeheimnis durch die §§ 17 ff UWG geschützt. Das UWG schützt das Betriebsgeheimnis nicht nur wegen seiner konstitutiven Bedeutung für die gesamte Wettbewerbsordnung, sondern auch wegen des kollektiven Interesses der Arbeitnehmer an der Erhaltung des Unternehmens. Abschließend ging der Referent auf den Transfer des strafrechtlichen Geheimnisschutzes in das Zivilrecht ein. Das Zivilrecht knüpft zivilrechtliche Folgen an die Verletzung der strafrechtlichen Geheimnisschutzvorschriften (§§ 3, 4 Nr. 11, 17 ff UWG; §§ 823 II BGB, 17 ff UWG). Zudem kann der Arbeitgeber an den Ermittlungsergebnissen der Strafverfolgungsbehörden teilhaben.

Der Kongreß endet mit der Verabschiedung.

Der diesjährige ZAAR-Kongress hat einen großen Beitrag zum bislang noch wenig diskutierten Know-How-Schutz geleistet. Professor Ann sowie Professor Rieble bedankten sich bei den Rednern für ihre hervorragenden Beiträge und den Teilnehmern für die angeregte Diskussion.

Abschließend wurde auf die 4. ZAAR-Tagung am 14. September 2012 in Hamburg hingewiesen.

Im Rahmen der ZAAR-Schriftenreihe werden die Vorträge und Diskussionen des 9. ZAAR-Kongresses in einem Tagungsband des ZAAR-Verlages erscheinen. Eine Übersicht der bisherigen Veröffentlichungen kann auf der ZAAR-Homepage unter der Rubrik „Verlag“ eingesehen werden.



Jennifer Junker
Wissenschaftliche Mitarbeiterin