David Ziegelmayer

Geheimnisschutz neu denken

In diesen Tagen steht ein scheinbar vergessenes Vorhaben der EU vor der ersten Lesung im EU-Parlament: Der Richtlinienentwurf zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen. Er könnte schon im Laufe des nächsten Jahres in Kraft treten – mit einschneidenden Folgen für die Branche.

Es gilt zunächst mit einem Missverständnis aufzuräumen: Beim Know-how-Schutz geht es nicht um schutzfähige Güter und Innovationen aus der Realwirtschaft wie etwa patentfähige Erfindungen. Betroffen sind vielmehr „weiche" Assets, über die jedes Unternehmen der Kreditwirtschaft verfügt: geschäftliche Vorhaben, geschäftspolitische Ziele, Ergebnisse von Geschäftsführer- und Aufsichtsratssitzungen, Beteiligungen, Fusionspläne, Kalkulationsunterlagen, Finanzierungspläne, Personaldaten, Markt- und Verkaufsstrategien sowie Absatz- und Werbemethoden, um nur einige Beispiele zu nennen. Und natürlich die Ausprägungen des rechtsgeschäftlichen Bankgeheimnisses, also persönliche Daten der Bankkunden samt deren Kreditwürdigkeit.

Allgemeiner Zugriff auf sensible Daten

Grob gesagt geht es um Dinge, die auf dem Markt „nichts zu suchen haben", was sich bis vor einigen Jahren bei Bankdaten quasi „von selbst" verstand. Die Branche muss sich nun aber nicht nur vor dem Hintergrund von zum Wirtschaftsgut avancierten CDs mit Kundendaten, die auf dem Markt erhältlich sind, oder dem Phänomen „Whistleblowing", das nicht immer rechtlich zulässig ist, fragen lassen, ob sie hier gut aufgestellt ist.

Daran kann man zweifeln: So meldete Morgan Stanley Anfang des Jahres, ein Mitarbeiter habe Daten von rund 350 000 Kunden gestohlen und einige davon im Internet veröffentlicht. Wie es dem Mitarbeiter gelungen war, an diese Daten zu gelangen „blieb zunächst unklar", wie die Frankfurter Allgemeine Zeitung meldete.

Aber auch hierzulande – das zeigt die Beratungspraxis – mangelt es nicht an Unternehmen, die schlicht über kein effektives Schutzkonzept verfügen: Mitarbeiter, die mit dem Kundenverkehr oder dem Vertrieb nicht in Berührung kommen, haben gleichwohl Zugang zu nahezu unendlich vielen Informationen. Die Aussage, dies sei „technisch nicht anders möglich" wird dabei nicht selten mit dem Hinweis gekoppelt, dass sich schließlich „jeder Mitarbeiter schriftlich zu Bankgeheimnis und Datenschutz verpflichtet" habe. Effektiver, interner Geheimnisschutz „hinter" dem gegenüber dem Kunden zu wahrenden Bankgeheimnis sieht anders aus.

Vernachlässigtes Thema

Es zeigt sich, dass das Thema in den vergangenen Jahren eher vernachlässigt worden und unter dem allgemeinen „Compliance-Radar" beinahe verschwunden ist.

David Ziegelmayer, Rechtsanwalt, Fachanwalt für gewerblichen Rechtsschutz, CMS Hasche Sigle, Köln.

Schon im kommenden Jahr kann eine neue EU-Richtlinie zum Know-how-Schutz in Kraft treten. Dann wird das Thema der sicheren Bewahrung von sensiblen Daten für Banken und Sparkassen in den Augen des Autors virulenter als bisher. Denn die deutsche Rechtsprechung sieht aktuell noch eine Vermutung des Geheimhaltungswillens vor. Das Erfordernis lautet nach seiner Meinung nun, Know-how und Geschäftsgeheimnisse zu klassifizieren und angemessen zu schützen. (Red.)

Die Wahrheit ist: Trotz eines allgemeinen Lamentierens über die Folgen von Wirtschaftsspionage kann in vielen Fällen von „angemessenen" Schutzmaßnahmen nicht die Rede sein.

Das dürfte sich bald ändern. Denn ein durchdachtes Know-how-Schutzkonzept – nicht die Ausflucht in Hinweise auf Datenschutz- und Complianceregeln – wird auch für viele Unternehmen der Kreditwirtschaft mit der EU-weiten Vereinheitlichung des Rechts „lebensnotwendig" werden. Die EU-Kommission sah hier bereits vor Jahren Handlungsbedarf, weil die aktuellen Regeln der Mitgliedsländer zum Schutz von Geschäftsgeheimnissen und Know-how heillos zersplittert sind. Jetzt nehmen die Bestrebungen Fahrt auf: Der entsprechende Richtlinienentwurf zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (COM 2013, 183) geht auf die Zielgerade und könnte zu Beginn des kommenden Jahres verabschiedet werden.

Vermutung des Geheimhaltungswillens

Dann dürfte sich die Rechtslage in Deutschland ebenfalls ändern. Denn der Entwurf sieht vor, dass der Abfluss von Unternehmensinterna in den Wettbewerb oder die Öffentlichkeit rechtlich nur dann zu verteidigen sein wird, wenn die Informationen eben durch „angemessene" Schutzmaßnahmen fremdem Zugriff entzogen wurden.

Bisher sieht die deutsche Rechtsprechung beim Geheimnisschutz noch eine Vermutung für einen Geheimhaltungswillen bei Unternehmen vor. Bei Anwendung der entsprechenden Vorschriften aus dem Gesetz gegen den unlauteren Wettbewerb (UWG) seien im Hinblick auf „die Manifes-

tation des Geheimhaltungswillens keine überzogenen Anforderungen" zu stellen. Mit anderen Worten: Der Geheimnischarakter von Unternehmensinterna ergibt sich sich aus der Natur der Sache. Wie gesagt: noch.

„Angemessene" Schutzmaßnahmen

Tritt die Richtlinie in Kraft, werden die Defizite im Know-how-Management spätestens dann offenbar, wenn etwa die Staatsanwaltschaft oder ein Zivilgericht, das das nationale Recht an dieser Richtlinie zu messen haben wird, fragt, wie der allgemeine Zugriff auf sensible Informationen etwa in einer Bank oder der laxe Umgang mit der Offenbarung von Interna gegenüber Geschäftspartnern mit dem Erfordernis der „angemessenen Schutzmaßnahmen" in Einklang zu bringen ist. Es steht zu erwarten, dass Unternehmen, die in diesem Moment ihr Konzept im Hinblick auf konkrete Geheimnisse nicht plausibel darlegen können, der Rechtsschutz gegen Spionage schlimmstenfalls komplett verwehrt wird. Die oben genannten Unternehmen, die hier pauschal auf technische Umstände und Mitarbeiterverpflichtungen verweisen, haben dann verloren.

Doch was sind „angemessene Schutzmaßnahmen"? Gemeint ist ein Konzept, das die im Voraus identifizierten und wirtschaftlich bewerteten Informationen vor internem und externem unbefugtem Zugriff schützt – und zwar nicht nur tatsächlich, zum Beispiel durch Zugangsbeschränkungen, sondern auch und vor allem rechtlich. Dazu zählen individuelle und konkrete Geheimhaltungsvereinbarungen, die in der bisherigen deutschen Praxis so gut wie nicht vorkommen.

Die Elemente eines solchen Schutzkonzepts müssen natürlich auf die Bedürfnisse des jeweiligen Unternehmens zugeschnitten werden. Eine rechtskonforme Umsetzung der Vorgaben, die die EU-Richtlinie vorsehen wird, wird sich in der Finanzbranche jedenfalls in folgenden Bereichen auswirken:

Klassifizierung der Geschäftsgeheimnisse

Zunächst müssen Zeit, Energie und Kosten auf die Ermittlung und Klassifizierung des Know-hows und der Geschäftsgeheimnisse eines Unternehmens verwendet werden. Die Herausforderung für das Informationsmanagement im Unternehmen wird es sein, Geheimnisse, Vorgänge und ja sogar bloße Ideen zu bewerten und zu klassifizieren.

Essenziell ist nach einer solchen Identifizierung und Bewertung die interne und externe Vertragscompliance. Sie muss auf den Prüfstand. Bisher übliche, pauschale „Vertraulichkeitsvereinbarungen/NDAs" mit Mitarbeitern, Dienstleistern, Partnern und Kunden werden im Lichte der Richtlinie keinen Bestand mehr haben. Betriebsgeheimnisse werden in Zukunft konkret bezeichnet werden müssen, um einen Minimum an wettbewerbsrechtlichem Schutz zu erreichen.

Die Kontrolle des Risikos der „eigenen Leute" erfolgt dabei zunächst über vertrauensbildende Maßnahmen mit dem obersten Ziel der Mitarbeiterzufriedenheit, aber eben auch und zwingend über das Arbeitsrecht. Schon zu Beginn muss nach dem „Need to know"-Prinzip der Zugang zu Informationen geregelt werden. Bei der Umsetzung ist die Einbindung der Personalabteilung in den Geheimnisschutz des Unternehmens durch Mitarbeiterauswahl, Optimierung und Nachführung von Arbeitsverträgen erforderlich.

Die üblichen Klauseln in Verträgen mit Arbeitnehmern, die sich auch nach dem Ausscheiden zur Verschwiegenheit verpflichten, sind – wenn nicht schon nach geltendem Recht – spätestens mit Umsetzung der Richtlinie wettbewerbsrechtlich wertlos. Auch hier werden Unternehmen nicht umhinkommen, Wissensträger zu identifizieren und notfalls über nachvertragliche Wettbewerbsverbote zur Geheimhaltung über konkret bezeichnete Geheimnisse zu verpflichten.

In Deutschland finden außerdem bislang nur ausnahmsweise sogenannte „Exit-Interviews" statt, die ausscheidenden Mitarbeitern eine Berufung auf „Gutgläubigkeit" nahezu unmöglich machen und in denen das Ende des Zugangs zu Unternehmensinformationen dokumentiert wird. Das ist notwendig, um gegebenenfalls nachweisen zu können, dass ein ausgeschiedener Mitarbeiter Informationen aus dem Unternehmen erst nach seinem Ausscheiden erlangt haben kann. Die „standardmäßige" Aufforderung zur Herausgabe von Unternehmenseigentum beim Ausscheiden ist dagegen wohl nicht mehr ausreichend.

Langfristiges Projekt

Auf der technischen Ebene liegt der Schutz von Mitarbeiter- und Kundendaten ebenso wie bloßer Ideen zu Geschäftsentwicklung und unternehmerische Entscheidungen gegen Externe – und zwar nicht nur auf IT- oder Datenschutzebene.

Im Falle des Geheimnisverrats oder der Betriebsspionage werden gerade Unternehmen der Finanzbranche schließlich über die Einhaltung eines den EU-Vorgaben genügenden Know-how-Schutzsystems genau wachen müssen: Nur wer den Abfluss von Know-how an Dritte bemerkt und sich dagegen wendet, verhilft den Unternehmensinteressen zum Durchbruch. Dazu gehört die Überwachung, Abmahnung und gegebenenfalls gerichtliche Inanspruchnahme von Wettbewerbern, die sich der Informationen eines Konkurrenzunternehmens bemächtigt haben.

Unter Compliance-Gesichtspunkten wird die Umsetzung der Vorgaben aus der EU-Richtlinie kein kurzfristiges Projekt sein. Sie erfordert eine Sensibilisierung der Mitarbeiter, bietet gleichzeitig aber auch die Chance, die Zusammenarbeit zwischen Rechts- und Complianceabteilungen mit den Fachabteilungen zu vertiefen und Geheimnisse dadurch effektiv zu schützen. Unternehmen, die nun handeln, werden dabei in Zukunft gestärkt aus etwaigen Auseinandersetzungen hervorgehen.

Siehe auch das Online-Tool der Kanzlei unter: ▶ http://know-how-protect.de