E-Compliance

(Referat gehalten beim Trivadis Knowledge and Network Event in Hamburg am 03. Juli 2008)
(Es gilt das gesprochene Wort)

von lic. iur. Patrik A. Häberlin, LL.M.

1. Das Urteil

Das Landgericht München I hat in einem Urteil vom 05. April 2007 entschieden, dass eine Vorstandsentlastung ohne Dokumentation des Risikofrüherkennungssystems nicht in Frage komme. Aufgrund von § 91 Abs. 2 Aktiengesetz hat der Vorstand geeignete Massnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit Entwicklungen, die den Fortbestand der Gesellschaft gefährden, früh erkannt werden. Das Gericht führte aus, dass die Einrichtung eines solchen Systems eine Organisationsanforderung zum Inhalt hat, der durch die Begründung unmissverständlicher Zuständigkeiten, einem engmaschigen Berichtswesen und einer entsprechenden Dokumentation Rechnung getragen werden kann und muss. Und es sei sicherzustellen – ich zitiere –, dass vom verantwortlichen Sachbearbeiter über die jeweiligen Hierarchieebenen bis hin zur Unternehmensleitung sämtliche relevanten Stellen von vorhandenen Risiken Kenntnis erlangen, um die entsprechenden Massnahmen zur Beherrschung dieser Risiken einleiten zu können. Das Risikomanagementsystem muss dokumentiert werden, um es auch unternehmensintern zu kommunizieren. Diese Offenlegung organisatorischer Regelungen, der getroffenen Massnahmen und Verfahrensabläufe trage nämlich entscheidend dazu bei, Handlungsabläufe innerhalb des Risikomanagementsystems einer Gesellschaft zu optimieren.

Interessant an diesem Entscheid ist, dass das Gericht mit aller Deutlichkeit darauf hingewiesen hat, dass die Dokumentation des Früherkennungssystems zu den **zentralen Aufgaben des Vorstandes** im Sinne von § 91 Abs. 2 AG und der damit verbundenen Bestandssicherungsverantwortung beiträgt.

Spätestens seit diesem Entscheid ist klar geworden, dass die E-Compliance oder IT-Compliance in zunehmendem Masse für alle Gesellschaften Gültigkeit hat. Und wenn man noch die amerikanische Compliance-Historie betrachtet, wird sie auch zunehmend an Bedeutung gewinnen. Es lohnt sich also, sich frühzeitig mit dieser Thematik auseinander zu setzen, wobei bereits an dieser Stelle gesagt werden kann, dass die E-Compliance auf der Vorstandsebene angesiedelt sein muss.

2. Compliance

a) Begriff

Compliance bezeichnet allgemein die Einhaltung verhaltenslenkender Normen durch eine Unternehmung. Dabei bedeutet Compliance nicht nur die Einhaltung von Gesetzgebung, Branchenstandards, Statuten, Weisungen usw., sondern auch ein ethisches Verhalten der Unternehmung im Sinne der Corporate Citizenship. Compliance hat überdies eine organisatorische Dimension und bezeichnet in diesem Sinne die Gesamtheit aller von einer Unternehmung getroffenen Massnahmen, die darauf abzielen, Regelverstösse durch die Unternehmung, ihre Organe und Mitarbeiter zu verhindern.

b) Entwicklung

Thematisch hat sich das Verständnis von Compliance in den letzten Jahren verändert. Ursprünglich war die Compliance auf den Bankenbereich fokussiert mit den Schutz- und Risikobereichen wie Insiderdelikte, Geldwäscherei usw. Von der damaligen punktuellen Betrachtung bestimmter Rechts- oder Tätigkeitsgebiete entwickelt sich die Compliance hin zu einer umfassenden Sichtweise, welche heute auch die Einhaltung kartell-, wettbewerbs-, arbeitsrecht-, immaterialgüter-, steuer- und umweltrechtliche Regeln umfasst, um nur einige Beispiele zu nennen[1]. E-Compliance ist also durch thematische Vielfalt geprägt und eine eigentliche Querschnittsaufgabe.

[1] U. Gasser/Daniel Markus Häusermann, E-Compliance, in Internet-Recht und Electronic Commerce Law, 9. Tagungsband, S. 73 f.

3. Die Querschnittsaufgabe

Im Prinzip können fünf zentrale Schutz- und Risikobereiche identifiziert werden, die im Visier der E-Compliance liegen. Selbstverständlich ist die genaue Bedeutung für das einzelne Unternehmen von der jeweiligen Branche, der Grösse des Unternehmens, dem Geschäftsmodell etc. abhängig ist. Im Einzelnen:

- Sicherheit
- Datenschutz
- Konsumentenschutz
- Immaterialgüter, insbesondere Urheberrecht
- Content Governance

Die Sicherung von Informationen und Informationssystemen erfordert technische, administrative und personelle Massnahmen, wobei auch die „Codes of Best Practice" von Branchen, Verbänden usw. zu berücksichtigen sind.

Bezüglich Datenschutz ist – zumindest in der Schweiz – eine Verschärfung der Bestimmungen zu beobachten. Auf den 1. Januar 2008 wurde in der Schweiz das Datenschutzgesetz geändert mit den zwei Hauptzielen, nämlich: erhöhter Schutz für Personendaten bei Online-Verbindungen und erhöhte Transparenz bei der Erhebung von Personendaten. Die Stellung der betroffenen Personen wird gestärkt, indem das geänderte Gesetz mehr Transparenz bei der Bearbeitung von Personendaten schafft, insbesondere durch die Einführung einer Informationspflicht gegenüber den betroffenen Personen beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. In Arbeit sind derzeit ausserdem Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem. Diese basieren in erster Linie auf der ISO-Norm 27001:2005. Man zielt darauf ab, ein Datenschutzmanagementsystem zu verlangen, was logischerweise ein Risikomanagement und - zwingend einhergehend - ein Konformitätsmanagement erfordert.

Von grosser Bedeutung in Deutschland ist zweifellos der Konsumentenschutz, der insbesondere im Bereich des E-Commerce eine bedeutsame Rolle spielt, etwa hinsichtlich der Zulässigkeit von Gerichtsstandsvereinbarungen und Rechtswahl, des

Vertragsschlusses, der inhaltlichen Gültigkeit sowie der Durchführung und Beendigung von Konsumentenverträgen.

Von zunehmender Bedeutung ist aber auch das Urheberrecht, wenn Sie beispielsweise an das Musik-Downloaden denken, an den Besuch von Peer-to-peer-Netzwerken oder an die Verlinkung von Websites. Je nachdem kann u.U. eine Haftbarkeit des Unternehmens gegeben sein, sei es, dass das Unternehmen selber die Links gesetzt hat oder beispielsweise Mitarbeiter die Downloads während ihrer Arbeitszeit tätigten.

Die Content-Governance ist zweifellos im Internet eines der Hauptknackpunkte, da die zivil- und strafrechtliche Verantwortlichkeit namentlich für Inhalte Dritter in den verschiedenen Ländern äusserst unterschiedlich sind. Hierauf kann nicht eingegangen werden, da es den Rahmen dieses Vortrages sprengen würde.

4. Die organisatorische Herausforderung

In der Schweiz haben wir in Art. 7 des Datenschutzgesetzes die gesetzliche Grundlage für ein umfassendes und ganzheitliches Sicherheitskonzept, das ein Unternehmen aufbauen muss. Es lautet ganz lapidar, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Verschärft wird diese Bestimmung durch Art. 9 der Verordnung zum Datenschutzgesetz, das die technischen, organisatorischen, personellen und letztlich auch baulichen Anforderungen an das Sicherheitsmanagement aufführt.

a) Verzahnung von Recht und Technologie

Immer mehr Geschäftsprozesse im Unternehmen sind heutzutage ohne Hilfe der Informationstechnologie gar nicht mehr möglich. Durch die Automatisierung und elektronische Abbildung der Geschäftsprozesse ist es mit einfachen Mitteln möglich, Informationen zugänglich zu machen und zu verteilen, doch diese Vereinfachung birgt auch ein hohes Risiko. Eben deshalb hat das Landgericht München I gestützt auf die Vorschrift des § 90 Abs. 2 Aktiengesetz darauf hingewiesen, dass die IT-Governance

zu den zentralen Aufgaben des Vorstandes im Sinne der Bestandssicherungsverantwortung gehört. In der Schweiz ist dies im Übrigen keineswegs anders. Eine ähnliche Regelung findet sich in Art. 716a Abs. 1 Ziff. 1 und 5 OR.

b) Risikomanagement

E-Compliance befasst sich nicht nur mit der Prüfung der Einhaltung von Rechts- und anderen verhaltenslenkenden Normen. Als weitere Funktionen fallen hier folgende Aufgaben in Betracht: Das aktive Verfolgen der rechtlichen, regulatorischen, technischen und marktlichen Entwicklungen; die Unterstützung beim Erlass interner Richtlinien und Weisungen (z.B. E-Mail-Policy); das Mitwirken bei der Entwicklung von Branchenstandards und Best Practices; die Information und Ausbildung von Mitarbeitern; das Ausarbeiten von Vorschlägen von organisatorischen Massnahmen; die Beratungstätigkeit im Falle konkreter Anfragen usw.

c) Auswirkungen auf die Unternehmensorganisation

Wie ich eben ausgeführt habe, ist die Sicherstellung von Compliance im Unternehmen in erster Linie eine organisatorische Herausforderung, die durch entsprechende organisatorische Massnahmen auf höchster Managementebene gestützt werden müssen. Dabei sind erst die Prozesse zu analysieren, danach können entsprechende Tools beschafft werden. Da aber durch die Compliance in einer nicht unerheblichen Art und Weise interne Ressourcen gebunden werden und entsprechende Kosten für die Implementierung und den fortlaufenden Betrieb anfallen, stellen sich viele Unternehmen der Komplexität der Anforderungen nur ungern. Wie Sie aber dem Entscheid des Landgerichtes München entnehmen können, kann eine verzögerte Implementierung zu empfindlichen Strafen wegen Nichteinhaltung der Vorschriften und dadurch zu noch höheren Kosten führen. Klar ist, dass Compliance das Zusammenspiel von Juristen und Technikern erfordert. Die gesetzlichen Anforderungen müssen in die Sprache des Unternehmens übersetzt werden, um daraus auch für Nichtjuristen verständliche Unternehmensrichtlinien ableiten zu können. Die IT-Verantwortlichen wiederum wandeln diese Unternehmensrichtlinien in konkrete Regeln für den Betrieb um, und sie sind für die Umsetzung und Einhaltung dieser Regeln verantwortlich. Das setzt

Vertrauen in die IT und deren entsprechende Umsetzungskompetenz voraus. Die Gesamtprozessvoraussetzung bleibt allerdings immer bei einer strategischen und übergeordneten Stelle.

5. Vorgehensweise zur Compliance-Umsetzung

Bei der Umsetzung der IT-Compliance sind in jedem Falle Unternehmensrichtlinien zu definieren, die

a) Benutzer/Benutzergruppen
b) Daten/Funktionen
c) Regeln/Berechtigungen
   definieren.

Zwar ist die Festlegung der Benutzer und Benutzergruppen immer unternehmensspezifisch, doch ist die Umsetzung der Berechtigungsmatrix immer wieder von den gleichen Modellen und Vorgehensweisen geprägt. Dabei darf aber die Komplexität des Themas und vor allem der organisatorische Aufwand nicht unterschätzt werden, der letztlich wesentlich höher ist als der technische.

Bei der Umsetzung der IT-Compliance kann folgendes Vorgehen zweckmässig sein:

a) Analyse der Gesetze
   - Prüfung auf Relevanz
   - Zuordnung zu Unternehmensbereichen
   - Priorisierung
   - Beachtung der Fristen

b) Richtlinien
   - Ableitung von Richtlinien aus dem Gesetz
   - Zuordnung zu Geschäftsprozessen
   - Zuordnung zu IT-Bereichen

c) Massnahmen für die Systeme
   - Ableitung von Massnahmen zur System- oder Datentrennung
   - Ableitung von Regeln für die Berechtigungsvergabe
   - Überprüfung der bestehenden Berechtigungsstruktur

6. Schluss

Die enge Verzahnung von Recht und Technologie, einer ausgeprägten Dynamisierung des Rechts, einer massiven Internationalisierung von Sachfragen und Rechtsproblemen sowie eine stark erhöhte Bedeutung von Soft Law erfordern eine Weiterentwicklung bestehender Compliance-Konzepte und eine Anpassung der entsprechenden Organisation. Wie bereits dargelegt, ist E-Compliance eine eigentliche Querschnittsaufgabe und eine Herausforderung für die Organe eines Unternehmens.