ecolex
FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT
JULI 2007
07
489–572

Vorsorgevollmacht

Register und Vertrauensschutz
Hürden im Liegenschaftsverkehr
Checkliste: Begriff – Form – Pflichten – Widerruf

Österr Bundesforste
Fruchtvöllerei statt Fruchtgenuss

Missbrauch beim
Squeeze-Out

Kronzeugenantrag auf
Erlass einer Kartellgeldbuße

Leibeigenschaft neu?
Flexibilisierung der Arbeitszeit

Verlustverwertung durch
Negativen Progressionsvorbehalt

RL-Teilumsetzung durch ein
Bundes-Umwelthaftungsgesetz

Gläubiger ohne Grenzen
Europäisches Mahnverfahren

MANZ

IT-Sicherheit und Haftung

Das Thema IT-Sicherheit (IT-Security) ist nicht nur ein technisches Spezifikum, sondern auch von großer unternehmerischer Relevanz. Der richtige Umgang mit IT entscheidet oftmals darüber, ob ein Unternehmen am Markt bestehen kann. Mangelnde IT-Sicherheit kann die Existenz des Unternehmens gefährden. Insofern wird IT-Sicherheit zum Inhalt der unternehmerischen Sorgfaltspflicht. Daher stellt sich auch die Frage nach der Haftung der verantwortlichen Organwalter (Geschäftsführer, Vorstand, Aufsichtsrat).

MICHAEL HASBERGER

A. Einleitung

Die Informationstechnologie[1]) hat Eingang in nahezu alle unternehmerischen Prozesse gefunden. Die eminente Bedeutung des sorgsamen Umgangs mit IT wurde nicht zuletzt durch Zusammenbrüche großer Unternehmen, wie etwa Enron, Worldcom, Health South, in den USA oder in Europa, Parmalat und Ahold, auch der breiten Öffentlichkeit ins Bewusstsein gerufen. Dabei kam es auch zu Haftungen der verantwortlichen Vorstandsmitglieder, da interne Kontrollprozesse versagten oder nicht ausreichend implementiert waren. Der Organwalter[2]) (zB Vorstandsmitglied, Mitglied des Aufsichtsrates, Geschäftsführer etc) hat gem § 347 UGB für die Sorgfalt eines ordentlichen Unternehmers einzustehen. Der Organwalter verfügt in der Regel nicht über das technische Fachwissen, um etwa eine dem technischen Stand der Technik entsprechende IT zu installieren, damit die erforderlichen Prozesse ordnungsgemäß ablaufen können. Er wird sich daher eines Fachmanns bedienen müssen, um den jeweiligen Anforderungen gerecht zu werden. Was entspricht nun der Sorgfalt eines ordentlichen Unternehmers in IT-Fragen?

B. Rechtliche Grundlagen

1. Internationaler Ansatz

Zu Beginn dieses Jahrtausends kam es in den USA zu spektakulären Unternehmenszusammenbrüchen und Insolvenzen, die auf ein mangelndes internes Kontrollverfahren in den einzelnen Unternehmen rückzu-

Dr. *Michael Hasberger* ist Partner der Hasberger_Seitz & Partner Rechtsanwälte GmbH in Wien.

1) Der traditionelle Begriff für diese Art der Technik lautet elektronische Datenverarbeitung (EDV). Vgl www.galileocomputing.de (Stand 4. 4. 2007).

2) Jene Person, die eine bestimmte Organposition einnimmt und ausübt. Vgl *Krejci,* Gesellschaftsrecht I (2005) 88 ff.

führen waren. All dies führte zum Sarbanes-Oxley Act (SOX).[3]) Im Rahmen der Sektion 404 des SOX müssen nunmehr Unternehmensprozesse genau beschrieben, definiert und Kontrollverfahren festgelegt werden, die das Risiko eines falschen Bilanzausweises minimieren sollen. Im Ergebnis wird damit die Verantwortlichkeit des Managements für Einrichtung, Effizienz und Nachvollziehbarkeit sowie Sicherheit der internen Kontrollprozesse bestimmt. Es lassen sich daraus – ohne Anspruch auf Vollständigkeit – bestimmte Erfordernisse, wie etwa für die Dokumentation von Prozessen und Kontrollen, Berechtigungsvergabe auf relevanten IT-Systemen, Kontrollen an den Schnittstellen, Datensicherheit sowie Datenbackups gewinnen.[4]) SOX gilt nur für den amerikanischen Jurisdiktionsbereich, hat allerdings darüber hinausreichende Ausstrahlungsfunktionen. So sind auch inländische Unternehmen, die an US-Börsen gelistet sind, sowie ausländische Tochterunternehmen börsennotierter US-Gesellschaften daran gebunden. Die Ausstrahlungsfunktion des SOX manifestiert sich allein darin, dass nunmehr auch die Europäische Union eine Richtlinie verabschiedete, die denselben Zweck wie SOX erfüllen soll.[5]) Daher wird nun auch für den europäischen Raum die Überwachung interner Kontrollsysteme und Risikomanagementsysteme zur vordringlichen Aufgabe. Wenngleich sich die Richtlinie inhaltlich mit der Rolle der Abschlussprüfer beschäftigt, wird auch die Verantwortung der Organwalter zur Überwachung insbesondere des internen Kontrollsystems, des internen Revisionssystems sowie des Risikomanagementsystems betont.[6])

Auch aus der vom Baseler Ausschuss für Bankenaufsicht erarbeiteten Rahmenvereinbarung (Basel II)[7]) lassen sich relevante Bestimmungen für IT-Security gewinnen.[8]) Demnach sollen bei der Entscheidung über die Kreditvergabe auch sog operationelle Risiken berücksichtigt werden.[9]) Letztlich können Defizite in der IT zu höheren Zinsen oder auch Kreditabsagen führen, sofern zB kein geeignetes Riskmanagement dokumentierbar oder Mängel bei der IT-Security erkennbar sind.

2. Nationaler Ansatz

a) Unternehmensrechtliche Bestimmungen

Für Organwalter in Leitungs- und Aufsichtsorganen in Erfüllung ihrer gesellschaftsrechtlichen Funktionen gilt § 347 UGB. Demnach haben die Organwalter für die Sorgfalt eines ordentlichen Unternehmers einzustehen. Nach herrschender Ansicht wird damit ein normativer Sorgfaltsmaßstab festgelegt, der je nach dem Leistungsstandard der betreffenden Berufsgruppe zu differenzieren ist, sodass branchenspezifische Übungen und Anschauungen zu berücksichtigen sind.[10]) Die Sorgfaltsanforderungen orientieren sich an der Sachverständigenhaftung nach den §§ 1299 f ABGB.[11]) Hingegen ist zu berücksichtigen, dass ein bestimmter haftungsfreier Spielraum für den Organwalter bleiben muss. Das unternehmerische Wagnis, dass die Chance auf Gewinn auch mit dem Risiko verbunden ist, Verlust zu erleiden, steht insofern in einem Spannungsverhältnis zu den unternehmerischen Sorgfaltspflichten. Jedenfalls ist der Organwalter dazu verpflichtet, die Grundlagen für seine Entscheidung sorgfältig zu ermitteln und sein Handeln danach auszurichten, das Unternehmenswohl zu fördern.[12])

Ähnliches gilt für die in den Materiengesetzen allgemein geregelten Sorgfaltspflichten von Organwaltern. Auch gem § 84 Abs 1 S 1 AktG hat jedes Vorstandsmitglied bei seiner Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.[13]) Auch hier gilt ein objektiver Maßstab, sodass der durch die Verkehrsauffassung bestimmte Begriff eines ordentlichen und gewissenhaften Geschäftsleiters in einem Unternehmen von der Art und dem Umfang, wie es dem konkreten Schadensfall zugrunde liegt, maßgeblich ist.[14]) Die sehr allgemein umschriebenen Sorgfaltspflichten verlangen nach einer Präzisierung. Hinweise dafür finden sich in § 82 AktG, der die Anforderungen des Vorstands für ein von ihm geleitetes Unternehmen konkretisiert, indem die Installierung eines entsprechenden Rechnungswesens sowie eines internen Kontrollsystems verlangt wird.[15]) Das Vorstandsmitglied ist daher organschaftlich verpflichtet, ein dem Stand der Technik entsprechendes Buchhaltungssystem (EDV) zu installieren. Bleibt das Vorstandsmitglied

3) http://fl1.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf (Stand 4. 4. 2007).

4) Sec 404. Management Assessment of International Controls.

5) Richtlinie 2006/43/EG des europäischen Parlaments und des Rates über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWR (8. EU-Richtlinie „Abschlussprüfer-RL"), ABl L 157 v 9. 6. 2006 S 87. Sie wurde am 17. 5. 2006 beschlossen und ist von den EU-Mitgliedstaaten bis 29. 6. 2008 in nationales Recht umzusetzen. Siehe auch Richtlinie 2006/46/EG des Europäischen Parlaments und des Rates, die seit Sommer 2006 in Kraft ist. ABl L 224 v 14. 6. 2006 S 1.

6) Vgl Kap 10 Art 41 (2) der RL 2006/43/EG.

7) www.oenb.at/de/presse_pub/period_pub/baselII/dokumente_basler/uebersetzdeutsch/uebersetzungen_der_deutschen_bundesbank.jsp#tcm:14–16831 (Stand 4. 4. 2007).

8) Die Umsetzung von Basel II in Europäisches Recht erfolgte durch RL 2006/48/EG des Europäischen Parlaments und des Rates v 14. 6. 2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute sowie RL 2006/49/EG des Europäischen Parlaments und des Rates v 14. 6. 2006 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten, ABl L 177 v 14. 6. 2006 S 1 sowie ABl L 177 v 16. 6. 2006 S 1. Zur Umsetzung in Österreich vgl Solvabilitätsverordnung (SolvaV) sowie die Offenlegungsverordnung (OffV) BGBl II 2006/374 bzw BGBl II 2006/375 sowie BWG-Novelle BGBl I 2006/141.

9) Operationelles Risiko ist die Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten. Diese Definition schließt Rechtsrisiken ein, beinhaltet aber nicht strategische Risiken oder Reputationsrisiken. Vgl Basel II Teil 2: V. Operationelles Risiko 157.

10) *Kramer* in *Straube,* HGB³ I § 47 Rz 4.

11) *Krejci,* Gesellschaftsrecht I (2005) 95.

12) *Krejci* (2005) 97 f und die dort zitierte E des BGH, ZIP 1997, 883.

13) Analog zur Haftung des Aufsichtsratsmitglied EvBl 1978/4. Sinngemäß § 25 GmbHG oder § 39 BWG. Vgl auch § 93 dAktG sowie § 43 dGmbHG.

14) *Strasser* in *Jabornegg/Strasser* AktG⁴ § 77 bis 84 Rz 95.

15) Vgl § 22 GmbHG. Der nähere Umfang dieser Verpflichtung ergibt sich auch aus den Bestimmungen des Steuerrechts (vgl §§ 124 ff BAO).

oder der Geschäftsführer untätig und entsteht daraus der Gesellschaft ein Schaden, so ist von einer Sorgfaltsverletzung auszugehen, die zur Haftung führen kann.[16])

Aus diesen Organisationsanforderungen (zB internes Kontrollsystem) lässt sich schließen, dass Maßnahmen zur Früherkennung von für das Unternehmen maßgeblichen Entwicklungen zu treffen sind sowie ein Überwachungssystem und ein allgemeines Risikomanagement vorhanden sein müssen. Dabei handelt es sich um Kernfunktionen der IT. Nur ein IT-System, dass diesen Erfordernissen entspricht, kann die Einhaltung dieser Organisationsanforderungen, für deren Umsetzung der Organwalter verantwortlich ist, gewährleisten.[17])

b) Sonstige Bestimmungen

§ 14 DSG 2000 normiert die Verpflichtung, im Falle der Datenverwendung umfangreiche Datensicherungsmaßnahmen zu treffen. § 14 Abs 2 DSG enthält den ausdrücklichen Auftrag, diese Datensicherungsmaßnahmen unter Berücksichtigung des Standes der Technik zu veranlassen. Daraus ergibt sich die unternehmerische Sorgfaltspflicht, in die Datensicherheit sowohl finanzielle als auch organisatorische Investitionen zu tätigen. Je schwieriger und umfangreicher die Datenanwendung ist, desto höher ist der Standard der Sicherheitsvorkehrungen zu veranlassen.[18]) Darüber hinaus normiert das DSG 2000 zahlreiche Tatbestände, die Handlungspflichten zu Lasten der Organwalter begründen.[19])

C. Rechtliche Würdigung

Aus zahlreichen Rechtsvorschriften lassen sich Pflichten des Organwalters ableiten, die den Sorgfaltsmaßstab eines ordentlichen und gewissenhaften Unternehmers iZm IT-Sicherheit konkretisieren. Ein Organwalter verhält sich nur dann ordentlich und gewissenhaft, wenn er für eine dem Stand der Technik entsprechende IT-Sicherheit sorgt. Nur so kann er für eine ständige Verfügbarkeit der Unternehmensdaten sowie für deren Unversehrtheit Gewähr leisten und den Erfordernissen eines internen Kontrollsystems nachkommen. Der Organwalter ist auch nach dem DSG 2000 dazu verpflichtet, für die Vertraulichkeit und die Sicherheit der Daten zu sorgen. Werden diese Maßnahmen nicht oder nur unzureichend umgesetzt, besteht grundsätzlich die Haftung des verantwortlichen Organwalters.[20])

16) Vgl BGH 20. 2. 1995, ZR 9/95 II. Der Geschäftsführer eines Unternehmens ist jedenfalls verpflichtet, sich über die gesamte wirtschaftliche Situation des Unternehmens einen Überblick zu verschaffen; dies auch, wenn das gesamte Buchhaltungs- und Finanzwesen ausgelagert wurde und sich die Geschäftsführung darum nicht ausreichend kümmerte.

17) Vgl *Hüffer,* Aktiengesetz[3] § 91 Rz 6 ff. Auch aus dem österreichischen Corporate Governance Kodex 2002 lassen sich Verpflichtungen zur Verfügungstellung eines funtionsfähigen Risikomanagements ableiten. Sofern es sich nicht ohnehin um gesetzliche Verpflichtungen handelt, sind diese Regeln nur dann von Relevanz, wenn diese den Stand der Technik iSd § 1299 ABGB wiedergeben. Vgl *Wilhelm,* The Austrian Corporate Governance Code – The Soft Persuader, ecolex 2003, 1.

18) *Knyrim,* Datenschutzrecht (2003) 228 f.

19) § 51 (Datenverwendung in Gewinn- oder Schädigungsabsicht); § 52 regelt Verwaltungsstrafen infolge rechtswidriger Datenverwendung; § 33 Schadenersatzpflicht infolge der Verletzung von schutzwürdigen Geheimhaltungsinteressen; § 1328 a ABGB immaterieller Schadenersatz bei Eingriff in die Privatsphäre des Betroffenen. Siehe auch § 5 ECG oder §§ 95 ff TKG 2003 (Sicherheit des Netzbetriebes, Datenschutz).

20) Es fehlt noch an Judikatur, die zum Thema IT-Sicherheit und Haftung herangezogen werden könnte. Vgl OLG Hamm, Urteil v 1. 12. 2003, 13 U 133/03. Dem kl Reiseunternehmen wurde mangels entsprechender Datensicherung das Alleinverschulden an einem Totalverlust der Daten zugeordnet. *Riedler,* Sicherheit in der Informationstechnik und Verantwortlichkeit, lex:itec 2006 (Ausgabe 04) 12.

SCHLUSSSTRICH

IT-Sicherheit ist von großer unternehmerischer Relevanz. Der verantwortliche Organwalter hat jedenfalls dafür zu sorgen, dass eine dem Stand der Technik entsprechende IT vorhanden ist, um die ständige Verfügbarkeit, die Vertraulichkeit sowie die Unversehrtheit der Daten zu gewährleisten, Unterlassungen führen zur Haftung für den dadurch verursachten Schaden.