Transatlantische Datenkontrolle

USA – EUROPA. *Ab Mitte April soll der Sarbanes-Oxley Act weltweit für Töchter amerikanischer Unternehmen gelten. Konflikte mit dem Datenschutz sind programmiert.*

VON RAINER KNYRIM UND VIKTORIA HAIDINGER

WIEN. Die Diskussion um Corporate Governance ist beinahe schon in einen Glaubenskrieg ausgeartet. Dabei blieben Sachfragen, wie eine Kontrolle von Unternehmen von innen und außen technisch und rechtlich konkret bewerkstelligt werden kann, weitgehend auf der Strecke. So etwa die Frage, wie sich im Hinblick auf die ab 15. April auch für Jahresabschlüsse nichtamerikanischer Unternehmen geltenden Kontrollpflichten des amerikanischen Sarbanes-Oxley Act der Widerspruch zwischen Kontrolle und Datenschutz lösen lässt.

Gehen die konzerninternen Kontrollbefugnisse etwa so weit, dass ein US-Mutterunternehmen einfach die gesamten Festplatten seiner österreichischen Tochter sicherstellen darf, selbst wenn darauf sensible Gesundheitsdaten von Österreichern gespeichert sind?

In den USA wurden erweiterte finanzielle Offenlegungspflichten und die Pflicht zur Einführung interner Kontrollsysteme durch den Sarbanes-Oxley Act gesetzlich geregelt. Der österreichische Corporate Governance Kodex enthält ebenfalls Hinweise auf ein interSCHWERPUNKT: Wirtschaft und Steuern §

nes Kontrollsystem. Obwohl datenschutzrechtliche Problemfelder offensichtlich sind, gehen weder der österreichische CGK noch der Sarbanes-Oxley Act darauf ein.

Die für die Kontrollsysteme zentrale Rechtsgrundlage ist Art. 404 des Sarbanes-Oxley Acts, der eine Verordnungsermächtigung für die Aufsichtsbehörde SEC enthält. Darin ist die Verantwortung des Managements vorgesehen, ein internes Kontrollsystem sowie jährlich eine verpflichtende Beurteilung von dessen Effektivität einzurichten. Die dazu ergangenen Regulations enthalten überwiegend unkonkrete Zielbestimmungen.

Der Sarbanes-Oxley Act wirkt nach der Vorstellung seines Gesetzgebers für Jahresabschlüsse ab dem

US-Präsident George W. Bush zelebrierte die Unterzeichnung des Sarbanes-Oxley Acts am 30. Juli 2002. [epa]

15. April 2005 extraterritorial: Sowohl ausländische Unternehmen, deren Aktien in den USA gehandelt werden, sollen erfasst sein als auch europäische Töchter von in den USA börsennotierten Unternehmen, sofern sie eine wesentliche Einheit der Muttergesellschaft bilden. Man möge sich den eingangs erwähnten, gewiss extremen Fall vorstellen, dass die US-Mutter einer in Österreich ansässigen Tochter die kompletten Festplatten der EDV der Tochter sicherstellen möchte und sich auf Art. 404 beruft.

Auf diesen Festplatten werden sich neben der Buchhaltung auch Kunden- und Lieferantendaten sowie dienstliche und allenfalls auch private Korrespondenz von Arbeitnehmern befinden, sodass Betroffene im Sinne des Datenschutzgesetzes hier nicht nur das Unternehmen, sondern ebenso der Arbeitnehmer selbst, Kunden und Lieferanten sowie (im Hinblick auf private Korrespondenz) unzählige dritte Personen sind. Ist das österreichische Unternehmen z. B. im Pharmabereich tätig, ist nicht auszuschließen, dass auch sensible Gesundheitsdaten auf den Festplatten gespeichert sind.

Bei der Berufung auf das US-Gesetz als Rechtsgrundlage für diese Daten-„Beschlagnahme", die wohl zu einer Datenübermittlung in die USA führt, stellen sich vor allem zwei Probleme: Erstens handelt es sich um ein ausländisches Gesetz, das in Österreich nicht direkt gilt, zweitens kann mangels Bestimmtheit nicht von einer – wie vom DSG verlangt – ausdrücklichen gesetzlichen Ermächtigung oder Verpflichtung gesprochen werden. Man könnte die Übermittlung vielleicht damit rechtfertigen, dass überwiegende Interessen des US-Mutterunternehmens vorliegen, die in Form von gesetzlichen Sorgfaltspflichten der Mutter im Konzern auf die Tochtergesellschaft wirken. Eine „pauschale" Übermittlung ganzer Festplatten mit allen personenbezogenen Daten in die USA wird sich aber auch damit kaum rechtfertigen lassen. Vielmehr müssten mit einer entsprechenden Software die Daten auf das zur Zielerreichung notwendige Maß reduziert werden.

Datenschutzkommission am Wort

Das Faktum der Datenübermittlung in die USA könnte überdies noch eine Pflicht zu deren Vorabgenehmigung bei der Datenschutzkommission auslösen, und es ist nicht anzunehmen, dass die Datenschutzkommission den Forderungen der US-Muttergesellschaft so rasch und einfach folgt, wie dieser im Ernstfall lieb wäre.

Ohne eindeutige Regeln können Unternehmen bei der Ausgestaltung konkreter Maßnahmen der Corporate Governance in eine Grauzone abgleiten – eine Zone, die zu verhindern die Corporate Governance gerade gedacht ist.

Die Brisanz des Themas wird durch das geplante Unternehmensstrafrecht verschärft: Unternehmen sollen strafbar sein, wenn Entscheidungsträger die nach den Umständen gebotene und zumutbare Sorgfalt außer Acht gelassen haben, insbesondere indem sie „wesentliche technische, organisatorische oder personelle Maßnahmen zur Verhinderung von Straftaten unterlassen haben". Auch hier würden die Unternehmen alleine gelassen bei der Entscheidung, was „nach den Umständen geboten ist" und wie sie Widersprüche zum Datenschutzrecht auflösen.

Dr. Rainer Knyrim ist Partner, Mag. Viktoria Haidinger, LL.M., Rechtsanwaltsanwärterin bei Preslmayr Rechtsanwälte, Wien.

„SOX": Reaktion auf Bilanzskandale

Der Sarbanes-Oxley Act, auch „Sox" genannt, wurde in den USA 2002 als Folge der Bilanzskandale um Enron oder Worldcom erlassen. Das Gesetz betrifft primär alle in den USA notierten Aktiengesellschaften, indirekt aber auch ausländische Unternehmen, die mit US-Konzernen verbunden sind. Ziel ist es, durch systematische Kontrollen die Gebarung der Unternehmen transparenter zu machen.

Corporate Governance ist seit den US-Skandalen auch in Europa in aller Munde. Gemeint ist der Ordnungsrahmen für die Leitung und Überwachung von Unternehmen. Mit Kodizes wie jenem in Österreich soll das Vertrauen von Anlegern gestärkt werden.

http: //news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf