ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT
JÄNNER 2009
01

1 – 100

Korruptionsstrafrecht

Energielenkung – Gehilfenzurechnung in der
Gaskrise

Unlauterer Wettbewerb qua
Kinder-Beeinflussung

Ministerialentwurf
Aktienrechts-Änderungsgesetz 2009

Entgeltbestimmung
Durch den Betriebsrat

Anrechnung von
Schul- und Studienzeiten

Rom II-VO für
Außervertragliche Schuldverhältnisse

MANZ

Outsourcing und Datenschutzrecht: Achtung, die Welt ist flach!

RAINER KNYRIM

Outsourcing ist einer der bedeutendsten wirtschaftlichen Trends des begonnenen 21. Jahrhunderts, wie nicht nur der Bestseller „Die Welt ist flach" von *Thomas L. Friedman*[1]) beschreibt, sondern auch die unternehmerische Praxis in Österreich zeigt: Täglich werden Datenanwendungen von österreichischen Unternehmen an Dienstleister im In- und Ausland, innerhalb oder außerhalb des eigenen Konzerns outgesourct, seien es Buchhaltung, Personalverrechnung, Mahnwesen, Marketing, technischer Support oder überhaupt der ganze Unternehmensserver. Schon vor einigen Jahren wurde an dieser Stelle darauf hingewiesen,[2]) dass bei Outsourcing nicht nur auf die physische und softwaremäßige Absicherung der Daten geachtet werden muss, sondern auch verschiedene formale Voraussetzungen erfüllt werden müssen. Auch wenn davon auszugehen ist, dass die physischen und softwaremäßigen Sicherheitsmaßnahmen heute besonders bei großen Dienstleistungsanbietern „State of the Art" sind (und § 14 DSG 2000 entsprechen), so überrascht der datenschutzrechtliche Zugang, mit dem an Outsourcingprojekte sowohl auf Auftraggeber- als auch auf Dienstleisterseite herangegangen wird, immer wieder aufs Neue. So wird zunächst oft übersehen, dass zwischen Auftraggeber und Dienstleister ein Dienstleistervertrag iSd § 10 Abs 1 DSG 2000 vereinbart werden sollte, dessen Mindestinhalt sich an § 11 DSG 2000 orientieren sollte:[3]) Selbst bei fingerdicken, hochdetaillierten Outsourcing-Verträgen und angehängten Service-Level-Agreements fehlen in der Praxis regelmäßig entsprechende Vertragsklauseln. Zu erheblichen Konsequenzen kann weiters das zum Teil völlige Ignorieren der Problematik des internationalen Datenverkehrs führen: Daten werden dem Dienstleister überlassen bzw diesem werden Datenzugriffe auf die Unternehmensdaten eingeräumt, ohne näher zu hinterfragen, wer beim Dienstleister von wo in der Welt die Dienstleistung erbringt. Einige Praxisfälle zur Illustration: Ein österreichisches Unternehmen lagerte die Buchhaltung an einen bekannten Datendienstleister aus und unterzeichnete einen Vertrag mit dessen tschechischer Konzerngesellschaft. Auf Nachfragen des Rechtsvertreters ergab sich, dass die Dienstleistung tatsächlich aber in Indien von einer anderen Konzerngesellschaft des Dienstleisters erbracht wurde. Zwei andere österreichische Unternehmen lagerten ihre Server jeweils in ihrer österreichischen Landeshauptstadt an dort ansässige „lokale" Dienstleister aus. Erst auf Insistieren des Rechtsvertreters stellte sich heraus, dass die Daten im einen Fall von Lateinamerika aus per Fernzugriff gewartet wurden, im anderen Fall in die USA zur Bearbeitung an mehrere Subdienstleister weiterverteilt wurden. Es überraschte, dass die Dienstleister kein datenschutzrechtliches Lösungskonzept für diese Fälle ausgearbeitet hatten, obwohl dies heute geradezu Standardsachverhalt ist und auch ihr eigenes „business model" waren. Dass bei solchen Outsourcingprojekten internationale Datentransfers vorkommen und eine entsprechende datenschutzrechtliche Aufarbeitung notwendig ist – etwa der Abschluss sog „Standardvertragsklauseln" zwischen Auftraggeber und Dienstleister oder die Einführung von „Binding Corporate Rules" und deren Genehmigung durch die DSK – wurde in der Lit bereits mehrfach aufgezeigt[4]) und sollte im Projekt auf beiden Seiten berücksichtigt werden. Dies auch, um nicht den Betriebsrat des Auftraggebers zu provozieren.[5]) Im fortschreitenden 21. Jahrhundert sollte auf beiden Seiten jedenfalls nicht übersehen werden, dass die Welt wieder flach geworden ist und die Daten meist schneller und häufiger auf dieser verteilt werden, als die Beteiligten es für möglich halten. Andernfalls könnte es beim Auftraggeber zu Projektmehrkosten, einer Projektverzögerung oder gar zu einem Projektstillstand oder -abbruch kommen.[6]) Der Dienstleister müsste sich spätestens dann die Frage nach einer möglichen Haftung für die mangelhafte Aufarbeitung seiner datenschutzrechtlich sehr relevanten internationalen Datenweiterleitungen oder -zugriffe stellen, allenfalls sogar wegen Verletzung vertraglicher (oder auch vorvertraglicher) Aufklärungspflichten aufgrund der nicht klaren Offenlegung derselben.

Dr. *Rainer Knyrim* ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte OG.

1) *Friedman,* The World is Flat: A Brief History of the Twenty-First Century (2005).

2) *Knyrim/Siegel/Autengruber,* Datenschutz und Datenrettung beim Outsourcing, ecolex 2004, 413.

3) Siehe näher dazu bei *Knyrim,* Datenschutzrecht 189 ff.

4) ZB *Knyrim,* Datenschutzrecht 202; *Knyrim,* Checkliste Zulässigkeit eines internationalen Datenverkehrs nach DSG 2000, ecolex 2002, 470; *Knyrim,* Neuerungen im Datenverkehr mit Drittländern, ecolex 2002, 466; *Sorger,* Übermittlung von Fluggastdaten in die USA, in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht und E-Government 2008, 191; *Dohr/Pollirer/Weiss,* DSG² Anm zu § 13.

5) § 96 a Abs 1 Z 1 ArbVG hält dazu fest, dass die „Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und *Übermittlung* von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzung hinausgehen" zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrats bedürfen. Im Hinblick auf die Definition von Übermitteln und Überlassen in §§ 4 Z 11 und 12 DSG 2000 wäre nur das Übermitteln von Daten im Sinne einer Weitergabe von Daten einer Datenanwendung an einen anderen Empfänger als den Betroffenen betriebsratszustimmungspflichtig, nicht jedoch das bloße Überlassen von Daten an einen Dienstleister. In der Praxis zeigt sich jedoch, dass gerade das in Konzernen häufig vorkommende konzerninterne Outsourcing auch von Mitarbeiterdaten an andere Konzerngesellschaften (zB Daten-Hosting der Human Resource-Daten am Server der Konzernmuttergesellschaft in Übersee) oftmals mit einer – dann betriebsratspflichtigen – Auswertung (= Übermittlung iSd § 4 Z 12 DSG 2000) der Daten im Eigeninteresse der Konzernmuttergesellschaft einhergeht.

6) Siehe insb § 52 Abs 4 DSG 2000.