ecolex
FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT
MAI 2004
05
337–424

Wettbewerb / Markenschutz / Freizügigkeit / USt

EU-Osterweiterung

§ 12a Abs 3 MRG

Machtwechseltheorie am Ende?

Die elektronische AG

Internet und Hauptversammlung

Gewährleistung für

Arbeitskräfteüberlassung

Steuerreform 2005 und

Unternehmensbesteuerung

Neu

Rechtsprechung Unabhängiger Finanzsenat

Datenschutz und -rettung beim

Outsourcing

MANZ

Datenschutz und Datenrettung beim Outsourcing

Outsourcing liegt bei Unternehmen stark im Trend. Immer weitere Unternehmensbereiche werden von externen Dienstleistern erledigt. Kaum ein Unternehmen denkt bei Outsourcing jedoch daran, unter welchen Bedingungen dieses datenschutzrechtlich zulässig ist und wie ein Unternehmen seine Daten in rechtlichen Krisensituationen retten kann.

RAINER KNYRIM / VOLKER SIEGEL / STEFAN AUTENGRUBER

A. EINLEITUNG

Outsourcing ist einer der bedeutendsten Trends bei der Unternehmensführung. Von der Buchhaltung über die Personalverrechnung zu Controlling, Mahnwesen, Marketing bis hin zur vollständigen physischen Verlegung aller Unternehmensserver zu einem Dienstleister – alles wird outgesourct. Der Trend hat Unternehmen jeglicher Größe erfasst, vom Einzelunternehmen bis zum Großkonzern wird ausgelagert, was ein Spezialist besser, billiger oder rascher erledigt.[1]) Fast immer ist mit dem Outsourcing auch eine Auslagerung der eigenen Daten verbunden, seien es Mitarbeiterdaten für die Personalverrechnung, Lieferantendaten für die Buchhaltung oder Kundendaten für Marketingaktionen. Unter welchen Voraussetzungen Outsourcing datenschutzrechtlich zulässig ist, wird dabei nur selten beachtet, obwohl das Datenschutzgesetz 2000 (DSG 2000) Outsourcing sogar ausdrücklich behandelt. Ebenso wenig überlegen die meisten Unternehmen, wie sie an ihre Daten gelangen, wenn ihr Dienstleister in Konkurs geht oder seine Leistung plötzlich nicht mehr erbringen kann oder will.

B. DIE DREI AKTEURE BEIM OUTSOURCING

Zunächst ist in Erinnerung zu rufen, dass es beim Outsourcing aus datenschutzrechtlicher Sicht drei

Dr. *Rainer Knyrim* ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte OEG. *Volker Siegel* ist Rechtsanwalt und Jurist bei NCC Escrow, München. Mag. *Stefan Autengruber* ist Leiter der Vertragsabteilung Region Central & Eastern Europe der SAP Österreich GmbH.

1) S die Entwicklung des Outsourcing in *Müthlein/Heck,* Outsourcing und Datenschutz[2] (1997) 3. Der Trend zum Outsourcen wird auch im Datenschutzbericht 2001 der Datenschutzkommission bestätigt (*Datenschutzkommission,* Datenschutzbericht 2001, 17, online unter http://www.bka.gv.at/datenschutz). S auch *Stempkowski,* Outsourcing – Realisierung eines Zusammenschlusstatbestandes? ecolex 2003, 920.

„Akteure" gibt, nämlich Betroffenen, Auftraggeber und Dienstleister.[2]) Betroffener ist der, dessen Daten verarbeitet werden, zB Kunde oder Mitarbeiter. Auftraggeber ist nach § 4 Z 4 DSG 2000, wer allein oder gemeinsam mit anderen die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob er die Verarbeitung selbst durchführt oder hiezu einen Dienstleister heranzieht. Dienstleister ist nach § 4 Z 5 DSG 2000, wer Daten, die ihm zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwendet.[3])

Bei Unternehmen ist organisatorisch zwischen internem und externem Outsourcing zu unterscheiden.[4]) Beim internen Outsourcing wird die Datenverarbeitung in einer Organisationseinheit (IT-Abteilung) geführt, deren Kosten transparent in einem eigenen Profitcenter erfasst werden. Durch die daraus entstehende Kostentransparenz stehen interne IT-Abteilungen oft in Konkurrenz mit externen Anbietern, die durch die Nutzung von Synergieeffekten oft günstigere Preise und ein besseres Service (zB 24 Stunden Hotline) anbieten können. Befindet sich die IT-Abteilung innerhalb derselben juristischen Person, ist die Überlassung der Daten an diese mE datenschutzrechtlich unproblematisch und ohne weitere Voraussetzung zulässig.[5]) Fungiert eine rechtlich selbständige Konzerngesellschaft als Dienstleister für eine andere, sind jedenfalls die Bestimmungen der §§ 10 und 11 DSG 2000 einzuhalten.

Die Unterscheidung, ob ein Dienstleisterverhältnis vorliegt oder nicht, ist aus zwei Gründen sehr wichtig: Erstens müssen dann, wenn Daten von einem Auftraggeber an einen Dienstleister weitergegeben werden, die strengen Voraussetzungen des § 7 Abs 2 DSG 2000 nicht erfüllt sein,[6]) denn es handelt sich in diesem Fall nicht um eine Übermittlung iSd § 7 Abs 2 DSG 2000, sondern um eine bloße Überlassung, für die das DSG 2000 diese Erleichterung vorsieht (s C.).[7]) Zweitens muss zwischen einem Auftraggeber und einem Dienstleister eine Dienstleistervereinbarung geschlossen werden (s D.).[8])

C. DATENSCHUTZRECHTLICHE ZULÄSSIGKEIT DES OUTSOURCING

Die Zulässigkeitsprüfung beginnt bei der Prüfung, ob die Datenschutzgrundsätze des § 6 DSG 2000 auch beim Outsourcing eingehalten werden[9]) und setzt sich mit der Frage fort, ob die Daten, die an den Dienstleister überlassen werden, davor zulässigerweise verarbeitet wurden. Denn wenn schon die Datenverarbeitung durch den Auftraggeber unzulässig war, dann ist umso mehr eine Datenüberlassung an den Dienstleister unzulässig.[10]) Damit die Datenverarbeitung an einen Dienstleister outgesourct werden kann, muss demnach zunächst deren Zweck und Inhalt vom Auftraggeber festgelegt werden, der Auftraggeber muss die rechtliche Befugnis für eine derartige Datenverarbeitung haben und es dürfen die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt sein, was va dann nicht der Fall sein wird, wenn der Betroffene der Datenverarbeitung zugestimmt hat, diese zur Erfüllung eines Vertragsverhältnisses mit dem Betroffenen notwendig ist oder der Auftraggeber gesetzliche Pflichten erfüllt.[11])

Sind diese Kriterien erfüllt, kann der Auftraggeber die Daten ohne weitere Prüfung dem Dienstleister überlassen, soweit dieser die Kriterien der §§ 10 und 11 DSG 2000 erfüllt; s dazu den nächsten Punkt. Eine weitere Prüfung, ob die Daten überlassen werden dürfen, wie dies bei Übermittlung an andere Auftraggeber nach § 7 Abs 2 DSG 2000 notwendig ist, muss nicht erfolgen, sofern die Überlassung der Daten innerhalb des Unternehmens, Österreichs oder der EU erfolgt.

Werden die Daten hingegen außerhalb der EU überlassen, so ist dieselbe Prüfung wie bei einer Übermittlung der Daten an einen Auftraggeber außerhalb der EU entsprechend §§ 12 und 13 DSG 2000 durchzuführen. Dies bedeutet, dass Datenüberlassungen an Dienstleister innerhalb der EU gegenüber Datenübermittlungen an Auftraggeber innerhalb der EU privilegiert sind, da innerhalb der EU für die Datenüberlassung keine Zustimmung des Betroffenen erforderlich ist. Bei Datenüberlassungen außerhalb der EU liegt diese Privilegierung nicht vor, bei diesen ist somit die Zulässigkeit ebenso zu prüfen wie bei Datenübermittlungen außerhalb der EU. §§ 12 und 13 DSG 2000 sehen eine Reihe von Möglichkeiten vor, die eine Datenüberlassung zulässig machen. Die wichtigsten materiellen Gründe sind das Vorliegen

2) Siehe auch die Erläuterungen zum „Datenschutzdreieck" in *Dohr/Pollirer/Weiss,* DSG², XXV ff.

3) Unterscheidungskriterium zwischen Auftraggeber und Dienstleister ist daher, wer über die Durchführung der Datenverarbeitung entscheidet: Trifft die Entscheidung der Auftraggeber und überlässt er die bloße Durchführung einem Dienstleister, so liegt ein Dienstleisterverhältnis vor. Wenn der Dienstleister die Daten aber für andere Zwecke weiterverarbeitet oder eigenständige Entscheidungen fällt oder sich nicht an den Auftrag des Auftraggebers hält, ist er hingegen nicht mehr Dienstleister, sondern wird selbst zum Auftraggeber.

4) Zusätzlich ist bei Unternehmen davor noch die Unterscheidung zwischen Auftraggeber und Dienstleister zu treffen, denn bei unternehmensinternen Dienstleistungsstellen zeigt sich oft, dass diese Daten(weiter)verarbeitung durchführen, deren Zulässigkeit gesondert geprüft werden muss.

5) Dies, weil § 4 Z 4 und 5 DSG 2000 formal auf die juristische Person als Einheit abstellen. Dagegen spricht allerdings, dass es nach § 4 Z 12 DSG 2000 auch Übermittlungen innerhalb eines Unternehmens gibt, woraus geschlossen werden kann, dass es auch Überlassungen im Unternehmen geben muss und dementsprechend argumentiert werden könnte, dass auch zwischen Unternehmensteilen derselben juristischen Person Dienstleisterverträge abzuschließen sind, was für Unternehmen aber einen kaum verständlichen und akzeptablen Aufwand bedeuten würde.

6) So ist – im Gegensatz zu vielen Fällen einer Datenübermittlung – bei der Datenüberlassung innerhalb der EU keine Zustimmung der Betroffenen einzuholen. *Knyrim,* Datenschutzrecht, Leitfaden für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm (2003) 115ff.

7) Dies ergibt sich aus § 4 Z 11 iVm § 7 Abs 2 DSG 2000.

8) §§ 10 und 11 DSG 2000.

9) Va der Zweckbindungsgrundsatz des § 6 Abs 1 Z 2 DSG 2000 und der Wesentlichkeitsgrundsatz des § 6 Abs 3 Z 3 DSG 2000 sollten beachtet werden. Näheres bei *Knyrim,* Datenschutzrecht 83 und 85.

10) § 7 Abs 1 und 2 DSG 2000.

11) *Dohr/Pollirer/Weiss,* DSG², Anm 8 bis 11 zu § 7; *Drobesch/Grosinger,* Das neue Österreichische Datenschutzgesetz (2000) 134; *Knyrim,* Datenschutzrecht 97 f; *Mayer-Schönberger/Brandl,* Datenschutzgesetz 2000 (1999) 19.

der Zustimmung der Betroffenen oder die Notwendigkeit zur Vertragserfüllung.[12]) Wichtige formelle Gründe sind die Gleichstellung des Drittstaates mit der EU in datenschutzrechtlicher Hinsicht (zB Schweiz, Ungarn, Kanada, Argentinien)[13]) oder der Abschluss der Standardvertragsklauseln für Auftragsverarbeiter.[14]) Ist keine dieser Möglichkeiten[15]) anwendbar, so muss die Datenüberlassung von der Datenschutzkommission genehmigt werden.

D. DIENSTLEISTERVERTRAG

Im vorigen Punkt wurde angemerkt, dass neben der Prüfung der Zulässigkeit der Datenüberlassung bei der Beauftragung eines Dienstleisters die Bestimmungen der §§ 10 und 11 DSG 2000 zu berücksichtigen sind. § 10 Abs 1 DSG 2000 sieht vor, dass ein Dienstleister nur dann in Anspruch genommen werden darf, wenn er ausreichende Gewähr für eine rechtmäßige und sichere Datenanwendung bietet und der Auftraggeber mit dem Dienstleister die hiefür notwendigen Vereinbarungen trifft. Der Auftraggeber haftet somit für das Auswahlverschulden des Dienstleisters. Um sich hier abzusichern, empfiehlt es sich, vom Dienstleister vor[16]) dessen Beauftragung die Vorlage eines Sicherheitskonzeptes[17]) zu verlangen, aus dem dessen technische und organisatorische Sicherheitsmaßnahmen ersichtlich sind (physischer und informationeller Hard- und Softwareschutz; Schutz der zu verarbeitenden Daten; Überwachung der Sicherheitsfunktionen; Auswahl der Mitarbeiter; Schulung der Mitarbeiter; Verpflichtung der Mitarbeiter zum Datenschutzgeheimnis; Überwachung der Mitarbeiter etc).

§ 10 Abs 1 DSG 2000 fordert weiters eine Vereinbarung zwischen Auftraggeber und Dienstleister, die zu Beweiszwecken am besten schriftlich getroffen werden sollte. Wenn die zwischen den Parteien vereinbarten Pflichten des Dienstleisters über dessen gesetzliche Pflichten hinausgehen (s den folgenden Punkt), ist Schriftlichkeit durch § 11 Abs 1 DSG 2000 ausdrücklich gefordert. Das wird in sehr vielen Fällen des Outsourcings vergessen, obwohl zwischen den Parteien regelmäßig sogar ein schriftlicher Vertrag über die Hauptleistung geschlossen wird (zB über eine Marketingaktion), in dem die Aufnahme der notwendigsten datenschutzrechtlichen Bestimmungen keinen großen Aufwand bedeuten würde. Werden die entsprechenden Klauseln nicht im Vertrag über die Hauptleistung eingefügt, wird, wenn überhaupt, meist ein stark an den Inhalt des § 11 Abs 1 DSG 2000 angelehnter „Dienstleistervertrag nach § 10 DSG 2000" schriftlich abgeschlossen.[18]) Je nach Belieben kann dieser Dienstleistervertrag die Dienstleisterpflichten näher ausformulieren, insb zur Klärung, ob der Dienstleister Subdienstnehmer grundsätzlich verwenden darf oder nicht, zur Überbindung gesetzlicher Geheimhaltungspflichten des Auftraggebers an den Dienstleister,[19]) zur Regelung, ob und in welcher Weise der Dienstleister die Auskunfts-, Richtigstellungs- und Löschungspflichten des Auftraggebers für diesen direkt wahrnimmt oder zur Klärung, ob der Dienstleister die Daten nach Beendigung der Dienstleistung vernichten, zurückgeben oder weiterverwahren soll. UU ist zur Absicherung des Auftraggebers gegen Missbrauch auch die Aufnahme einer Vertragsstrafe bei Verstößen des Dienstleisters sinnvoll. Hält der Dienstleister den Dienstleistervertrag dann nicht ein, kann er mehrfach zur Verantwortung gezogen werden, nämlich vom Auftraggeber aus der Vertragsstrafe und allenfalls darüber hinausgehendem Schadenersatz nach Zivilrecht wegen Vertragsbruchs[20]) und, wenn der Vertragsbruch gleichzeitig einen Verstoß gegen die gesetzlichen Pflichten des § 11 Abs 1 DSG 2000 bedeutet, zusätzlich nach den Verwaltungsstrafbestimmungen des § 52 DSG 2000[21]) durch die zuständige Bezirksverwaltungsbehörde.

E. DIENSTLEISTERPFLICHTEN

Nach § 11 Abs 1 Z 1 DSG 200 hat der Dienstleister die Pflicht, die Daten ausschließlich im Rahmen des Auftrags des Auftraggebers zu verarbeiten; andernfalls würde er selbst zum Auftraggeber.

Der Dienstleister hat nach § 11 Abs 1 Z 2 DSG 2000 weiters die Datensicherheitsmaßnahmen des § 14 DSG 2000 einzuhalten. Dies, damit durch die Auslagerung der Datenverarbeitung an einen Dienstleister keine Lücke im vom Gesetz geforderten Datenschutzniveau entsteht. Zusätzlich muss der

12) § 12 Abs 3 Z 5 und 6 DSG 2000.

13) Ebenso US-Unternehmen, die sich den „safe harbor"-Regeln unterworfen haben. *Dohr/Pollirer/Weiss,* DSG², Anm 12 zu § 13; *Knyrim,* Neuerungen im Datenverkehr mit Drittländern, ecolex 2002, 466.

14) *Bond/Knyrim,* Data Protection – Third Country Transfers, Computer Law and Security Report, 2002, 187; *Dohr/Pollirer/Weiss,* DSG², Anm 8 zu § 13; *Knyrim,* Datenübermittlung in Drittländer: Standardvertragsklauseln der Europäischen Union, AnwBl 2001, 65.

15) Siehe sämtliche Möglichkeiten in *Knyrim,* Checkliste: Zulässigkeit eines Internationalen Datenverkehrs nach DSG 2000, ecolex 2002, 470. Künftig wird es nach Entwürfen der Europäischen Artikel 29 Datenschutzgruppe zusätzlich auch noch die Möglichkeit geben, die gesamte Konzerndatenverarbeitung durch Konzerndatenschutzrichtlinien genehmigen zu lassen. Diese Möglichkeit ist in Österreich schon umsetzbar. *Knyrim,* Multinationals offered respite from strict EU data-transfer rules, World eBusiness Law Report 24. 7. 2003.

16) Auch während der Durchführung der Dienstleistung muss der Auftraggeber die Einhaltung des Vertrages überprüfen, insb dann, wenn er Zweifel an dessen Einhaltung hat. *Damman/Simitis,* EG Datenschutzrichtlinie, Kommentar (1997) 230.

17) *Drobesch/Grosinger,* Datenschutzgesetz 148; *Dohr/Pollirer/Weiss,* DSG², Anm 4 zu § 14.

18) Siehe zB den Mustervertrag der Datenschutzkommission unter http://www.bka.gv.at/datenschutz. Solch ein Vertrag ist ein Vertrag sui generis, der aber – va im Hinblick auf Schadenersatzmöglichkeiten bei Vertragsbruch – wie ein Werkvertrag unter normales Zivilrecht fällt. *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 2000 (2000) 56.

19) ZB ärztliche Schweigepflicht (§ 54 ÄrzteG), Bankgeheimnis (§ 38 BWG).

20) *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 56.

21) Va wegen eines Verstoßes gegen § 52 Abs 1 Z 2 DSG 2000, wenn der Dienstleister eigenmächtig übermittelt oder verarbeitet sowie gegen § 52 Abs 2 Z 4 DSG 2000 bei gröblicher Missachtung der Datensicherheitsbestimmungen des § 14. Auch der Auftraggeber selbst kann strafbar werden, wenn er zB einen Dienstleister außerhalb der EU beauftragt, ohne vorher eine allfällig notwendige Genehmigung der Datenschutzkommission dafür einzuholen (§ 52 Abs 2 Z 2 DSG 2000) oder wenn er wegen der Auswahl eines schlechten Dienstleisters nicht im Stande ist, seinen Offenlegungs- oder Informationspflichten nach §§ 23 ff nachzukommen (§ 52 Abs 2 Z 3 DSG 2000).

Dienstleister seine Mitarbeiter zur Einhaltung des Datengeheimnisses des § 15 DSG 2000 verpflichten. Im Dienstleistervertrag sollten die weiteren gesetzlichen Verpflichtungen hinsichtlich der Zulässigkeit der Beauftragung von Sub-Dienstleistern[22]) und der Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflichten[23]) näher ausgestaltet werden. Jedenfalls näher geregelt werden sollte im Dienstleistervertrag oder durch spätere Anordnungen, ob der Dienstleister am Ende seiner Arbeit die Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, entweder dem Auftraggeber zurückgeben oder in dessen Auftrag für ihn weiter aufbewahren oder vernichten soll.[24])

Der Dienstleister unterliegt der Prüfhoheit des Auftraggebers, denn er muss dem Auftraggeber jene Informationen zur Verfügung stellen, die zur Kontrolle der Einhaltung der vorgenannten Verpflichtungen notwendig sind.[25])

F. KÜNFTIGEN DATENZUGRIFF ABSICHERN

Sind die Daten einmal zulässigerweise outgesourct, stellt sich die Frage, wie der Auftraggeber auch künftig Zugriff auf die Daten erhält. In Problemfällen, wie zB Insolvenz des Dienstleisters, Leistungsverweigerung des Dienstleisters oder schlichte Unmöglichkeit seiner Leistung, zeigt sich, dass ein gut ausgestalteter Dienstleistervertrag zwar ein hilfreicher Ansatz sein mag, um rechtliche Ansprüche auf die Daten zumindest theoretisch abzusichern;[26]) einen sofortigen tatsächlichen Zugriff auf die an den Dienstleister ausgelagerten Daten wird der Auftraggeber damit aber nicht erlangen.

Bei der Entwicklung von Software besteht eine ähnlich gelagerte Problematik, da va bei Individualsoftware beim Konkurs des Programmierers bzw des Softwarehauses das Risiko sehr hoch ist, dass der Auftraggeber mit der Software nichts mehr anfangen kann, da ihm der Quellcode („Source Code") fehlt, um die Software weiter zu warten oder zu entwickeln. Mit Hilfe von Treuhandvereinbarungen, „Escrow-Agreements" genannt,[27]) lässt sich uU eine geeignete Absicherung für den Weiterbetrieb der Software bei Insolvenz oder Nichterfüllung des Softwareunternehmens erzielen.[28]) Escrow-Agreements sehen vor, dass der „Source Code" bei einem Treuhänder (Escrow-Agent) hinterlegt wird, der bei Eintritt des vordefinierten Treuhandfalles den Source Code an den Auftraggeber herausgibt.[29])

Unternehmen achten bei Abschluss von Softwarelieferungs- oder Kaufverträgen oder beim Abschluss von Outsourcing-Vereinbarungen zwar darauf, einen straffen Leistungskatalog zu definieren und eine Source Code-Hinterlegung mittels Escrow-Agreement zu vereinbaren, vergessen in der Praxis meist aber völlig, an die mit der Software verarbeiteten Daten zu denken. Mit den gängigen Escrow-Agreements mag zwar der Fortbetrieb der Software gesichert sein, dies wird aber in vielen Fällen nutzlos sein, da die *mit* der Software verarbeiteten Unternehmensdaten durch ein typisches Escrow-Agreement *nicht* gesichert sind. Die Software hat nämlich rechtlich und vertraglich mit den Daten nichts zu tun und ist auch physisch von diesen getrennt. Dies lässt sich am einfachen Beispiel eines Mobiltelefons verdeutlichen: Dieses besteht aus dem Gerät, der zu dessen Betrieb notwendigen Software und der SIM-Karte des Telefonnetzbetreibers, auf der die Rufnummer als Datum gespeichert ist. Fehlt die Rufnummer

22) § 11 Abs 1 Z 3 DSG 2000.

23) § 11 Abs 1 Z 4 DSG 2000. Die Auskunfts-, Richtigstellungs- und Löschungspflichten sind in §§ 26 f DSG 2000 geregelt.

24) § 11 Abs 1 Z 5 DSG 2000.

25) § 11 Abs 1 Z 6 DSG 2000.

26) Die Frage, inwieweit ein solcher Dienstleistervertrag insolvenzfest ist, gäbe Stoff für einen eigenen Beitrag und kann in diesem Rahmen nicht weiter erörtert werden, sollte aber unbedingt beachtet werden.

27) Zu Escrow-Agreements s ua *Karger,* Software-Hinterlegungsverträge, in *Kilian/Heussen,* Computerrechtshandbuch (2001) Z 36; *Kast/Meyer/Wray,* Software Escrow, CR 2002, 379; *Schneider,* Neues zu Vorlage und Herausgabe des Quellcodes? CR 2003, 1 ff; *Siegel,* Software Escrow – die konkreten Anforderungen an eine Quellcodehinterlegung in der Praxis, CR 2003, 941.

28) Auch die tatsächliche rechtliche Konkursfestigkeit solcher Escrow-Agreements nach der österr Rechtsordnung kann an dieser Stelle nicht näher untersucht werden. Siehe zur dt Rechtsmeinung zB *Oberscheidt,* Die Insolvenzfestigkeit der Softwarehinterlegung, Schriften zum Informations-, Telekommunikations- und Medienrecht (2002); *Paulus,* Insolvenzverfahren, Sanierungsplan: Risiken und Vermeidungsstrategien, CR 2003, 237 ff.

29) *Bartsch,* Softwarehinterlegung, Beck'sches Formularhandbuch Bürgerliches-, Handels- und Wirtschaftsrecht (2003); *Nordman/Schumacher,* Escrow-Agreement: Softwarehinterlegung in der Praxis, K & R 1999, 363; *Schneider,* Handbuch des EDV-Rechts[3], M 114 ff und Anh IX mit Vertragsmuster.

auf der SIM-Karte, nützt weder das Gerät noch dessen Software etwas. Ein weiteres einfaches Beispiel: Was hilft der modernste elektronische Terminkalender mit den vielfältigsten Anwendungsmöglichkeiten, wenn alle Termine in diesem gelöscht sind?

Datensicherung ist bei Unternehmen nur bei der eigenen Datenverarbeitung üblich, nicht jedoch beim Outsourcing. Unternehmen müssen daher überlegen, wie in Krisenfällen nicht nur der Weiterbetrieb der Software sichergestellt werden kann, sondern gleichzeitig auch der Zugriff auf die eigenen, outgesourcten Daten. Als Lösung bietet sich an, entweder vom Dienstleister regelmäßig Datenbackups auf CD-Rom einzufordern oder die Datenträger regelmäßig treuhändig bei einem Dritten zu hinterlegen, so wie es auch mit dem Source Code geschieht. Der Datenbestand wird dabei aber nie aktuell sein. Mittlerweile gibt es bereits Dienstleister, die reine Datensicherungsservices (Backup-Services) anbieten und im Notfall mit mobilen Servern an ein Netzwerk „andocken" können, um verloren gegangene Daten aus externen Backups wieder einzuspielen. Diese werden üblicherweise aber nur zur eigenen Absicherung eingesetzt, wenn ein Unternehmen seine Daten selbst verarbeitet. Wenn das Unternehmen seine Datenverarbeitung outsourct, sollte der Dienstleister im Dienstleistervertrag zu umfangreichen Datensicherungsmaßnahmen verpflichtet werden, allenfalls durch das Backup-Service eines Subdienstleisters. Auch dann fehlt dem auftraggebenden Unternehmen wahrscheinlich aber noch immer der freie Zugriff auf die Daten, da es bei einem Ausfall des Dienstleisters technisch keinen Zugriff auf die Daten und zum Subdienstleister keine vertragliche Beziehung hat. Die optimale Lösung zur Datensicherung bei Outsourcing dürfte sein, in die Vertragsbeziehung mit dem Dienstleister zusätzlich ein externes Realtime-Backup-Service einzubinden, das mit dem auftraggebenden Unternehmen direkt einen Vertrag schließt, der jederzeitigen Zugang zu den Daten gewährt oder den externen Backup-Servicedienstleister zumindest verpflichtet, den Zugangscode zu seinen Daten bei einem Escrow-Agent zu hinterlegen, damit der Auftraggeber bei Ausfall des Dienstleisters die Möglichkeit hat, rasch an seine beim externen Backup-Service gesicherten Daten zu gelangen.

SCHLUSSSTRICH

Unternehmen müssen beim Outsourcing nicht nur die datenschutzrechtlichen Voraussetzungen wie den Abschluss eines Dienstleistungsvertrages beachten, sondern auch den künftigen Zugriff auf die eigenen Daten rechtlich und faktisch absichern.