jusalumni Magazin

03/2009

„Datenschutzrecht ist eine grundrechtlich hoch sensible Rechtsmaterie“

Veränderung im Umgang mit Wissen

Neue Kommunikationsformen bilden sich heraus

Im Gespräch:
Univ.-Prof. Dr. Gabriele Kucsko-Stadlmayer

Datenschutz im Arbeitsverhältnis
ao. Univ.-Prof. Dr. Martin E. Risak

Datenglobalisierung
Dr. Rainer Knyrim

Recht und Datenschutz

P.b.b. Verlagspostamt 1030 Wien,
GZ 05Z036471M
Einzelheft: € 6,50; Jahresabo: € 24,–

Elektronische Aufzeichnungen und Datenglobalisierung

Datenschutzrechtsexperte Dr. Rainer Knyrim im Gespräch mit dem jus-alumni Magazin

Ob Personalverrechnung, Buchhaltung, Mahnwesen, Marketing, technischer Support oder überhaupt der ganze Unternehmensserver: Die unternehmerische Praxis in Österreich zeigt, dass laufend Datenanwendungen ins In- und Ausland outgesourct werden. Im Datenschutzrecht gibt es allerdings noch keinen globalisierten Datenverkehr. Es ist daher verboten, Daten ohne Weiteres rund um die Welt zu schicken.

Herr Dr. Knyrim, was ist beim Outsourcing von Dienstleistungen zu beachten?
Dr. Rainer Knyrim: Als erstes ist auf die Verpflichtung aus dem Datenschutzgesetz zu achten, dass man Dienstleisterverträge abschließen muss. Das ist bei jeder Dienstleistung der Fall und wird sehr oft übersehen. Ich habe schon hundertseitige Verträge (Service-Level-Agreements) gesehen, in denen Datenschutz nicht einmal mit einem Satz erwähnt wird. Zu regeln ist etwa, dass sich der Dienstleister an seine Aufträge halten muss, seine Mitarbeiterinnen und Mitarbeiter schult und Datensicherheitsmaßnahmen setzt. Ebenso wird die Frage geklärt, was nach Beendigung der Dienstleistung mit den Daten passiert, nämlich ob sie vernichtet, aufbewahrt oder sie zurückgegeben werden sollen.

Gelten unterschiedliche Vorschriften für den internationalen Datenverkehr?
Im internationalen Datenverkehr – über die EU-Grenzen hinaus – gibt es eine Besonderheit. Hier ist zu beachten, wo man die Daten hinschickt. Einige Länder sind mit der EU gleichgestellt, wie etwa Argentinien und Kanada. Ein Vertragsabkommen zwischen der EU-Kommission und dem US-Handelsministerium, die sogenannten Safe Harbor-Richtlinien, regeln das Erfassen, Verwenden und Speichern persönlicher Daten aus der Europäischen Union. Ein amerikanisches Unternehmen kann sich auf der Website http://www.export.gov/safeharbor/ registrieren und somit öffentlich machen, dass es ein „sicherer Hafen" für europäische Daten ist. Andernfalls muss ein Vertrag abgeschlossen und bei der österreichischen Datenschutzkommission vorher zur Genehmigung eingereicht werden. Dafür gibt es Muster von der Europäischen Kommission, die sogenannten Standardvertragsklauseln.

Das klingt nach einem langwierigen Verfahren.
Bei Dienstleistungen ist es meist nicht mehr so langwierig; wir schaffen es mittlerweile in drei bis vier Monaten. Allerdings ist das ein Zeitraum, der in Projekten zu beachten ist, denn

diese werden auf wirtschaftlicher Seite oft lange im Voraus geplant, rechtlich jedoch oft nicht. Nach der Unterzeichnung möchte man rasch die Arbeit aufnehmen. Wenn man sich erst zu diesem Zeitpunkt überlegt, was hinsichtlich des Datenschutzes zu tun ist, kann es zu einer Projektverzögerung kommen. Wenn man es überhaupt vergisst, dann hat man ein Problem. Dies merke ich häufig bei österreichischen Gesellschaften großer Konzerne, die die Daten irgendwo um die Welt schicken und erst sehr spät bemerken, dass das nicht ohne Weiteres zulässig ist.

Wie lauten die Strafbestimmungen?
Es drohen nach dem Datenschutzgesetz Geldstrafen bis max rund EUR 19.000,–, was für einen großen Konzern verschmerzbar sein dürfte. Das große Risiko ist aber, dass die Verwaltungsbehörde gleichzeitig den „Verfall" von Datenträgern und Programmen aussprechen kann, also quasi den Entzug der betroffenen IT, was für ein Unternehmen zu einer Art „Supergau" werden könnte. Im Übrigen ist auch schon der Versuch strafbar, Datenschutzverstöße sind daher keine Kavaliersdelikte.

Um welche Daten geht es? Was wird hauptsächlich globalisiert?
Es geht um sämtliche personenbezogene Daten, hauptsächlich und typischerweise um Mitarbeiterdaten und um Kundendaten. Die Globalisierung von Kundendaten ist insofern heikel, als man sich überlegen muss, ob man die Zustimmung des Kunden braucht oder mit überwiegend berechtigtem Interesse dafür argumentieren kann, dass diese jemand anderer irgendwo auf der Welt weiterverwenden kann. Auch bei Mitarbeiterdaten ist Achtsamkeit gefordert. Dabei muss allenfalls der Betriebsrat eingebunden werden oder in betriebsratslosen Unternehmen die Zustimmung der einzelnen Arbeitnehmer. Das ist dann gar nicht Datenschutzrecht, sondern Arbeitsverfassungsrecht. Wenn es sich um eine reine Speicherung im Ausland handelt, dann ist das Verfahren meistens nicht so langwierig. Problematisch ist auch oft ein internes Outsourcing, wenn etwa eine Konzernmutter den zentralen Server für alle Konzerngesellschaften in den USA stehen hat und dort alle Daten auf eine zentrale Personalverwaltungssoftware gelegt werden, oder wenn ein Server in der Nacht nicht in Salzburg, sondern aus Costa Rica oder wo zur gleichen Zeit die Sonne scheint, gewartet wird. Möglicherweise könnte jemand aus dem Konzern versuchen, sich die Daten anzusehen, weil er oder sie gerne wissen will, was die Beschäftigten in Österreich leisten und wie viel Geld sie dafür bekommen. Das ist dann keine Dienstleistung mehr, sondern eigentlich wie eine Übermittlung an einen fremden Dritten. Im Datenschutzrecht gibt es nämlich kein Konzernprivileg. Es ist daher verboten, Daten ohne Weiteres um die Welt zu schicken.

Eigentlich eine unerwartete Restriktion im Zeitalter der Globalisierung?
Das ist historisch bedingt. Das österreichische Datenschutzgesetz wurde Ende der 1970er-Jahre, die EU-Datenschutzrichtlinie Anfang der 1990er-Jahre entwickelt und hinken daher der Realität nach. Die Konzerne haben sich durch die Globalisierung erst ab den 1990er-Jahren EDV-technisch stark vernetzt. Heute gibt es immer wieder intensive politische Diskussionen, die zum Ziel haben, die EU-Datenschutzrichtlinie zu ändern und zu modernisieren. Auf der anderen Seite stehen Gewerkschaften und Konsumentenschützer, die sagen, dass nicht alles so vernetzt sein soll. Seit rund zwei Jahren erlebe ich in diesem Zusammenhang auch verstärkt, dass Betriebsräte sehr gut geschult sind und dadurch sogar häufig besser informiert sind, als die Juristen und Geschäftsführer in den Unternehmen, die dadurch unter Druck kommen.

Das heißt, die Unternehmen wünschen sich eine Öffnung?
Ja, absolut. Der ganz große Trend – eine Folge der Globalisierung – ist, dass die Konzerne alle ihre Daten irgendwo zentralisieren und Datenbanken vereinheitlichen möchten. Es macht ja auch keinen organisatorischen oder wirtschaftlichen Sinn, in jedem Land eine andere Software zu verwenden. Arbeitnehmervertretern gefällt es naturgemäß jedoch nicht so gut, wenn Daten konzernweit vernetzt werden und etwa jemand in Indien die Gehaltsverrechnung macht oder die Konzernzentrale in Übersee viele private Informationen über die Beschäftigten hat.

Welche Entwicklungen sind aktuell verstärkt zu beobachten?
Unternehmen überwachen ihre Mitarbeiterinnen und Mitarbeiter immer häufiger. Sie werden mit Videokameras aufgezeichnet und durch Zutritts- und Zeiterfassungssysteme kontrolliert. Beispielsweise hat der OGH die Speicherung personenbezogener Daten, nämlich biometrischer Merkmale, als Kontrollmaßnahme iSd §96 Abs 1 Z 3 ArbVG beurteilt, die geeignet ist, die Menschenwürde zu berühren. Die Interessen der Mitarbeiter am Schutz ihrer Privatsphäre wiegen schwerer als das „vergleichsweise triviale Ziel" der Kontrolle der Kommens- und Gehenszeiten. Daher war in diesem Fall laut OGH die Zustimmung des Betriebsrats zur Einführung eines solchen Systems zwingend einzuholen.

Welche Varianten von elektronischen Aufzeichnungen gibt es noch?
Elektronische Personalakten sind der neueste Trend. Was man früher in Papier vor Ort hatte, ist heute in einem elektronischen Personalakt unter Umständen plötzlich weltweit verfügbar. Mitarbeitergespräche werden nicht mehr unter vier Augen, sondern elektronisch geführt und mittels Web-Formularen erledigt. Mitarbeiterbeurteilungen oder -schulungen werden „virtuell" über das Internet durchgeführt. Bei den elektronischen Mitarbeitergesprächen zeigt sich zunächst ein Problemfeld, dass in internationalen Konzernen von Land zu Land eine andere Fragekultur vorherrscht, weshalb die Beurteilung von Soft Skills oft nur sehr allgemein und vage erfolgt. Die Auswirkungen des zeitversetzten Bearbeitens müssen ebenso hinterfragt werden. Die Rechtsprechung der Datenschutzkommission zu elektronischen Mitarbeitergesprächen und -beurteilungen ist allerdings noch sehr spärlich.

Anlässlich der Veröffentlichung des Fotos des Diebes der „Saliera", das

aus der Videoaufzeichnung eines Handyshops stammte, war die Zulässigkeit von Videoüberwachung plötzlich in aller Munde. Wie ist die aktuelle Rechtslage?
Datenschutzrechtlich sind Videoüberwachungsanlagen, sofern sie die Videobilder aufzeichnen, vorab bei der Datenschutzkommission zu genehmigen. Sie lösen nämlich eine Vorabgenehmigungspflicht nach § 18 Abs 2 Z 1 und 2 DSG 2000 aus. Videobilder können sensible Daten etwa über die ethnische Herkunft (zB Hautfarbe) oder den Gesundheitszustand (zB Rollstuhlfahrer) oder aber voraussichtlich enthaltene strafrechtlich relevante Daten (zB aufgezeichneter Diebstahl) enthalten. Es gibt jedoch unterschiedliche Meinungen, weshalb abzuwarten bleibt, ob sich an der Genehmigungspflicht etwas ändern wird.

Gibt es auch eine Verpflichtung, gespeicherte Daten eine gewisse Zeit lang aufzuheben oder auch herauszugeben?
Alle Betroffenen haben nach § 26 DSG ein Auskunftsrecht und können einen Ausdruck der Daten erhalten und die Information, wer darauf Zugriff hat. Wenn die Auskunftspflicht nicht binnen acht Wochen erfüllt wird, kann sich der oder die Betroffene sofort mit einer Beschwerde an die Datenschutzkommission wenden. Diese wickelt ein Beschwerdeverfahren ab, das mit einem Bescheid endet, der dann vor dem Verwaltungsgerichtshof angefochten werden kann.

Jede und jeder Betroffene kann auch dagegen klagen, dass ihre oder seine Daten überhaupt verarbeitet werden. Man kann auch auf Löschung klagen, das muss allerdings vor einem Zivilgericht geschehen, was aufgrund des Kostenrisikos den Rechtszugang ein bisschen erschwert. Eine Auskunftsklage bei der Datenschutzkommission ist hingegen kostenlos.

Herzlichen Dank für das Gespräch!

Dr. Rainer Knyrim ist Partner bei Preslmayr Rechtsanwälte und überdies Mitglied der "Task force on Privacy and the Protection of Personal Data" der Internationalen Handelskammer (ICC) Paris und der Deutschen Gesellschaft für Recht und Informatik.

Weiters ist er wissenschaftlicher Beirat der Zeitschrift jusIT (Zeitschrift für IT-Recht, Datenschutz und Rechtsinformation von LexisNexis) und Mitglied des Programmkomitees des Österreichischen IT-Rechtstages des Forschungsvereins für Informationsrecht und Immaterialgüterrecht.