25 Jahre Datenschutzrecht in Österreich

von **Rainer Knyrim**

Bestandsaufnahme und Lösungsansätze für aktuelle Probleme[1])

Das Jahr 2005 ist ein Dreifach-Jubiläum für den Datenschutz. Vor 25 Jahren, am 01.01.1980, trat das erste österreichische Datenschutzgesetz[2]) in Kraft. Vor zehn Jahren, am 24.10.1995, wurde die Europäische Datenschutzrichtlinie[3]) beschlossen. Seit fünf Jahren, nämlich seit dem 01.01.2000, gilt das DSG 2000[4]) in Österreich. Dieser Beitrag soll einige der trotz dieser langen Geschichte des Datenschutzrechts nach wie vor bestehenden Probleme als „Bestandsaufnahme" zeigen und Lösungsansätze bringen. Insbesondere wird der Frage nachgegangen, ob selbstregulierende Maßnahmen eine Lösung dieser Probleme bringen könnten.

1. Grundsätzliche Probleme des Datenschutzrechts in seinem 25. Jahr des Bestehens

Zunächst sei ein Grundproblem des Datenschutzrechts im Allgemeinen aufgegriffen: In den Rechts- und Wirtschaftsstudien erfolgt noch immer praktisch keine Ausbildung im Datenschutzrecht, ebenso wenig wie dies in der späteren Berufsausbildung der Fall ist. Es ist sehr verwunderlich, dass sogar in der weiteren Berufsausbildung der „klassischen" Juristen das Thema Datenschutzrecht so gut wie nicht vorkommt. Daraus resultiert eine breite Unkenntnis der – leider ziemlich komplexen – Materie Datenschutzrecht in Wirtschaft, Verwaltung, aber auch der Justiz selbst.[5]) Folgeproblem dieser Unkenntnis ist einerseits die „Vogel-Strauß-Politik" gegenüber dem Datenschutzrecht als Passivreaktion – man steckt den Kopf in den Sand und hofft, dass nichts passiert. Andererseits ist es dadurch möglich, dass oft als aktive Überreaktion gegen unliebsame Projekte das Datenschutzrecht als „Keule" geschwungen wird. Mit dieser „Datenschutzkeule" werden Projekte schlicht „erschlagen", ohne dass auf einer sachlichen Ebene über eine rechtlich oft mögliche Lösung diskutiert wird.

Ein anderes Problem ist, dass die österreichische Datenschutzkommission im Vergleich zu anderen Datenschutzbehörden in Europa über wenig Personal verfügt, was sich auf die Verfahrensdauer erheblich auswirkt. Dass sich Beschwerdeverfahren gegen Unternehmen entsprechend hinziehen, mag für manche Unternehmen ein angenehmer Effekt dieser Situation sein. Tatsächlich trifft dies aber viele Unternehmen sehr negativ, nämlich dann, wenn sie sich um Genehmigungen internationaler Datentransfers bemühen oder der Erledigungen ihrer Meldungen beim Datenverarbeitungsregister harren und oft viele Wochen oder Monate warten müssen, bis sie die Gewissheit haben, dass ihre Datenverarbeitung oder -übermittlung akzeptiert wird. Dies ist im schnelllebigen Informationszeitalter ein ernsthaftes Problem für Unternehmen, die ihre IT-Infrastruktur verändern. Obwohl die wenigen Mitarbeiter der Datenschutzkommission und des Datenverarbeitungsregisters extrem bemüht und entgegenkommend sind,[6]) können fehlende Mittel durch noch so viel Engagement nicht völlig wettgemacht werden. Die Datenschutzkommission selbst spricht in ihrem Datenschutzbericht 2005 eine sehr deutliche Sprache über ihre Situation, die sie als „unhaltbar" bezeichnet. In einem europäischen Vergleich rangiert die österreichische Datenschutzkommission (mit dem Verhältnis von einem Mitarbeiter zu 400.000 Einwohnern) auf Platz 24 von 31 europäischen Ländern.[7])

Am 5. Juli 2005 hat die EU-Kommission gegen die Republik Österreich ein Vertragsverletzungsverfahren wegen mangelhafter Umsetzung der Datenschutzrichtlinie eingeleitet. Laut EU-Kommission sei die „völlige Unabhängigkeit" der Datenschutzkommission nicht gewährleistet, einer der Gründe könnte die finanzielle Abhängigkeit von bzw. Nichtausstattung mit finanziellen

RA Dr. Rainer Knyrim, Preslmayr Rechtsanwälte OEG, Wien

1) Dieser Beitrag ist eine überarbeitete „Langversion" eines Referates bei der zweiten Tagung des „Vereins zur Förderung des Medien- und Informationsrechts an der WU-Wien (MIR)" zum Thema „Datenschutz durch marktwirtschaftliche Instrumente – Funktioniert eine 'regulierte Selbstregulierung'?". Eine Zusammenfassung sämtlicher Referate der Tagung wurde bereits von *Philapitsch*, Selbstregulierung im Datenschutz – Bericht von einer Diskussionsveranstaltung an der Wirtschaftsuniversität Wien, MR 2005, 270 publiziert.

2) Das Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz), BGBl 565/1978, stammt tatsächlich sogar schon vom 18. Oktober 1978.

3) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995, ABl L 281 v 23.11.1995, 31.

4) Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl 165/1999.

5) Bis zum Obersten Gerichtshof, dessen Urteil 4 Ob 50/04p vom 4.5.2004 für Verwunderung in der Literatur gesorgt hat, siehe *Knyrim*, Kann man sich zum Schutz seiner Kundendaten nicht mehr auf das DSG 2000 berufen?, ecolex 2004, 873; *Jahnel*, OGH: Kein Schutz von Unternehmensdaten nach dem DSG, RdW 2005, 200; *Dohr/Pollirer/Weiss*, Datenschutzrecht² E 5 zu § 4.

6) Der Verfasser kann aus eigener Erfahrung sogar über am Sonntag (!) von Mitarbeitern der Datenschutzkommission an ihn versandte E-Mails berichten.

7) Datenschutzbericht 2005 der Datenschutzkommission (Berichtzeitraum 1. Jänner 2002 bis 30. Juni 2005, online abrufbar unter www.dsk.gv.at).

Mitteln durch den Staat sein.[8]) Kein Grund zum Jubeln im Jubiläumsjahr – es bleibt zu hoffen, dass daraus entsprechende Konsequenzen gezogen werden.

2. Probleme des Datenschutzrechts in Unternehmen

Konsequenz der eingangs geschilderten Nichtwissensproblematik ist, dass Datenschutzrecht vorwiegend (nur) in Unternehmen betrieben wird, in denen geschulte Personen damit betraut sind oder zumindest das „Gespür" haben, wann ein Thema datenschutzrechtliche Implikationen hat und diesen nachgegangen werden sollte. Dort, wo sich in einem Betrieb jemand im Datenschutzrecht auskennt und sich um dessen Einhaltung sorgt, könnte auch eine Selbstregulierung stattfinden. Eine Überlegung wäre daher, die betrieblichen Datenschutzbeauftragten ähnlich wie in Deutschland[9]) – aber auf freiwilliger Basis – im Datenschutzgesetz zu verankern. Dies ist derzeit in Österreich – regelmäßig sogar zur Verwunderung von Unternehmen, die an betriebliche Datenschutzbeauftragte in den Konzerngesellschaften zB in Deutschland selbstverständlich gewöhnt sind[10]) – nicht der Fall. Die Ausstattung der betrieblichen Datenschutzbeauftragten mit gewissen Rechten, aber auch Pflichten, hat nach Aussage der deutschen Datenschutzbehörden[11]) einen sehr positiven Effekt gehabt.

Ein anderes Problem des Datenschutzrechts in Unternehmen ist, dass Unternehmen mit dem Argument, dass in Österreich kaum Strafen[12]) zu befürchten seien, dieses schlicht ignorieren, obwohl erhebliche rechtliche Risken bestehen, denen sich viele Unternehmen aber aufgrund ihrer Unkenntnis einfach nicht bewusst sind. Erst kürzlich hat in Deutschland – wo die Rechtslage ähnlich ist – zB die Nichteinbindung der Betriebsräte und die Missachtung datenschutzrechtlicher Bestimmungen zu einem vorübergehenden Totalstopp eines bereits in Implementierung befindlichen großen Personaldatenverarbeitungssystems der öffentlichen Hand geführt.[13]) Auch in Österreich kann die Nichtgenehmigung zB des Transfers der Daten einer österreichischen Tochtergesellschaft in eine konzernweite, internationale Datenbank[14]) durch die Datenschutzkommission zum ernsthaften faktischen Problem werden, da dies eine „Zwangsisolierung" von der Datenstruktur – und somit letztlich der EDV-Struktur des eigenen Konzerns – zur Folge haben kann.[15]) Fast niemandem ist überdies bekannt, dass die Datenschutzkommission bei Beschwerden gerade in jüngster Zeit bei Unternehmen vor Ort durch das „Zentrum für sichere Informationstechnologie-Austria (A-SIT)" als Amtssachverständigem Augenscheine durchführen und Gutachten erstellen hat lassen.[16])

Motivation für die Beschäftigung mit Datenschutzrecht ist für viele Unternehmen vor allem die Furcht vor negativer Publicity in den Medien, sei es durch Anprangerung durch datenschützende Institutionen wie den Verein für Konsumenteninformation, die ARGE Daten, die jährlich vergebenen „Big Brother Awards" oder die allgemeinen Medien. Erst wenige Unternehmen[17]) haben erkannt, dass die Bewerbung der eigenen Datenschutzkultur auch aktiv für positive Publicity genutzt werden könnte. Eine Förderung aktiver Datenschutzkultur etwa durch standardisierte Audits oder Gütesiegel, wie dies etwa in Deutschland geschieht,[18]) wäre ein auch in Österreich wünschenswerter Ansatz, der im Hinblick auf eine verstärkte Selbstregulierung sehr positive Effekte hätte.

Ein weiteres Problem des Datenschutzrechts in Unternehmen und gleichzeitig eines der Grundprobleme der Selbstregulierung im Datenschutzrecht in Österreich ist, dass der gegen Auftraggeber des privaten Bereichs wegen Verletzung der Rechte des Betroffenen auf Geheimhaltung, Richtigstellung oder auf Löschung sowie auf Schadenersatz (§§ 32 und 33 DSG 2000) Rechtssuchende auf den „normalen" Zivilrechtsweg verwiesen wird (Klagen sind beim örtlich zuständigen Landesgericht für Zivilrechtssachen einzubringen).[19]) Dies reduziert die Bekämpfung von „Miniverstößen" oder auch größeren Fällen von Datenschutzrechtsverletzungen durch den Betroffenen. Welches Unternehmen oder welche Privatperson bringt auf volles eigenes Kostenrisi-

8) Der Standard, 11. August 2005.

9) Neben Deutschland haben auch Frankreich, Luxemburg, die Niederlande, Schweden und die Slowakei Datenschutzbeauftragte in verschiedenen Gestaltungsformen, siehe die Übersicht in *Klug*, Internationalisierung der Selbstkontrolle im Datenschutz, RDV 2005, 163 (165).

10) *Klug*, Internationalisierung der Selbstkontrolle im Datenschutz, RDV 2005, 163 (167) meint richtig, dass es bei den betrieblichen Datenschutzbeauftragten nicht nur um die Einhaltung von Datenschutzgesetzen, sondern vielmehr auch um Kunden- und Mitarbeiterzufriedenheit geht.

11) Siehe Arbeitspapier Nr. 106 vom 18.1.2005 der Artikel 29 Datenschutzgruppe, downloadbar unter http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf.

12) Dass die Datenschutzkommission bei erheblichen Datenschutzbedenken auch medienwirksam tätig wird, hat der Fall „Herold Marketing CD-Rom private" gezeigt, siehe Presseaussendung der Datenschutzkommission vom 4.12.2003, downloadbar unter http://www.dsk.gv.at sowie *Knyrim*, Data Protection Commission investigates marketing CD-Rom, World eBusiness Law Report, 4.11.2003.

13) Beschluss des Verwaltungsgerichtes Wiesbaden vom 04.10.2004, GZ 23 LG 511/05 (V), siehe http://www.jurpc.de/rechtspr/20040279.htm, aufgehoben durch B des Hessischen Verwaltungsgerichtshofes vom 10.6.2005 GZ 22 TH 1497/05 (nicht veröffentlicht).

14) Siehe zur Rechtslage in Deutschland *Hilber*, Die datenschutzrechtliche Zulässigkeit intranet-basierter Datenbanken internationaler Konzerne, RDV 2005, 143ff.

15) Zu den unbeachteten Problemen etwa beim Outsourcing siehe *Knyrim/Siegel/Autengruber*, Datenschutz und Datenrettung beim Outsourcing, ecolex 2004, 413.

16) ZB E DSK vom 7.6.2005, K120.813/006-DSK/2005, E DSK vom 21.6.2005, K120.839/005-DSK/2005, E DSK vom 10.5.2005 K120.908/0009-DSK/2005, E DSK vom 26.11.2004, K120.911/0014-DSK/2005.

17) Siehe zB Daimler Chrysler, die mit dem Motto „Premium cars, premium services, premium privacy" ihre Datenschutzkultur als zusätzliches Verkaufsargument verwenden. „Daimler Chrysler Codes of Conduct", downloadbar unter http://www.daimlerchrysler.de unter „Datenschutz".

18) § 9a BDSG.

19) Näheres bei *Knyrim*, Datenschutzrecht (2003), 223 ff.

ko eine Klage vor dem Landesgericht ein, weil es zB eine datenschutzrechtlich unzulässige Werbesendung erhalten hat? Welches Unternehmen bringt eine datenschutzrechtliche Klage ein, weil ein anderes Unternehmen es mit datenschutzrechtlich unzulässiger Erlagscheinwerbung belästigt?[20]) In Summe können eine große Anzahl solcher einzelner „Miniverstöße" für den Verstoßenden einen erheblichen Vorteil bringen, indem zB ein Unternehmen bewusst bei groß angelegten Werbeaktionen gegen das Datenschutzrecht verstößt, in der Erwartung, dass sich der einzelne Empfänger nicht die Mühe und das Kostenrisiko einer Klage antun wird (insbesondere wenn er nach den allgemeinen zivilrechtlichen Regelungen aufgrund von § 33 DSG 2000 vermutlich Probleme haben wird, einen Schaden nachzuweisen). Diese Situation scheint zunächst ein Vorteil für Unternehmen zu sein, da diese, sofern sie nicht grundsätzlich die ethische Einstellung zum rechtlich richtigen Handeln haben und sich vor negativer Publicity fürchten, durchaus kalkuliert Datenschutzverstöße in größerem Ausmaß begehen können, ohne dass ihnen etwas „passiert", da die Datenschutzkommission nach § 31 DSG 2000 bei Privatunternehmen nur für Verstöße gegen die Auskunftspflicht[21]) zuständig ist und derartige Fälle regelmäßig auf den Zivilrechtsweg verweisen.[22]) Der Nachteil für Unternehmen und die Wirtschaft im Allgemeinen ist aber, wie dargestellt, dass betroffene Unternehmen Datenschutzverstöße ebenfalls auf gerichtlichem Weg durchsetzen müssen. Davor scheuen diese oft zurück, sowohl wegen des Kostenrisikos, als auch wegen der erheblichen Rechtsunsicherheit mangels Judikatur zu diesem Thema. Diese Situation hilft somit letztlich den „schwarzen Schafen" und schadet den Unternehmen, die sich wohl verhalten.

Der „direkte" Klagsweg über §§ 32 und 33 DSG 2000 ist den meisten Unternehmen aufgrund der aufgezeigten Umstände durchwegs fremd, bekannt ist vielen Unternehmen aber das Wettbewerbsrecht. Durch die „Hintertür" des Wettbewerbsrechts kommt in letzter Zeit verstärkt das Datenschutzrecht herein. *Jahnel/Thiele*[23]) haben erst kürzlich aufgezeigt, wie Datenschutzrecht als UWG-rechtliche „Waffe" eingesetzt werden kann. Ein Unternehmen, das bemerkt, dass ein Konkurrent ihm sein Geschäft dadurch wegnimmt, dass die eigenen Kundendaten – auf welchen Wegen auch immer – zu diesem gelangen und ausgewertet werden oder dass von Konkurrenten datenschutzrechtlich unzulässige Werbeaktionen (zB durch unzulässige Datenverknüpfungen oder unzulässigen Datenaustausch zwischen Unternehmen)[24]) durchgeführt werden, wird heute nicht mehr lange zögern, das Datenschutzrecht in einem UWG-Prozess als Argument für einen Gesetzesverstoß, der zu einem Wettbewerbsvorteil (Gewinnung von Marktanteilen) verwendet wird, einzusetzen. Das Datenschutzrecht als marktwirtschaftliches Selbstregelungsinstrument liegt also im Trend, fraglich ist aber, ob UWG „die" Lösung ist, um Datenschutzrecht weiterzuentwickeln und vor allem, um Selbstregulierung im Datenschutzrecht zu betreiben. Es sollte überlegt werden, ob nicht den Betroffenen ein verbesserter Zugang zum Datenschutzrecht geschaffen werden sollte. Immerhin handelt es sich beim Datenschutzrecht um ein verfassungsrechtlich gewährleistetes Grundrecht mit unmittelbarer Drittwirkung[25]) und unter das Datenschutzrecht fallen in Österreich – im Gegensatz zu den meisten anderen Ländern der Welt – nicht nur die Daten natürlicher Personen, sondern gleichermaßen auch die Daten von Unternehmen.[26])

Ein völlig anderes, europaweites Problem ist, dass es in der EU trotz einer einzigen Datenschutzrichtlinie 25 im Detail recht unterschiedliche Datenschutzgesetze sowie 25 Datenschutzbehörden gibt, die diese unterschiedlich handhaben. Dies, obwohl die Datenschutzrichtlinie eigentlich zum Ziel hatte, den freien Datenverkehr innerhalb der Europäischen Union zu ermöglichen.[27]) Als Beispiel sei die simple Definition einer „Zustimmung" genannt. So ist die Zustimmung („Einwilligung") nach Art 2 lit h Datenschutzrichtlinie „jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden". Tatsächlich gibt es in praktisch jedem Mitgliedsstaat der Europäischen Union aber zusätzlich zu dieser Definition weitere gesetzliche oder judizielle Ausformungen dieser Zustimmung, sei es im Hinblick auf die Einholung (konkludent, ausdrücklich, schriftlich, unmissverständlich) oder die Widerruflichkeit oder die Gültigkeitsdauer.[28])

---

20) Ein derartiger Fall war Gegenstand einer Beschwerde bei der Datenschutzkommission, die in der Hauptsache auf den Zivilrechtsweg verwies, siehe *Knyrim*, Hosting von Websites (§ 16 ECG) ist Dienstleistung im datenschutzrechtlichen Sinn, MR 2004, 51.

21) Wie wenig sowohl Unternehmen als auch die öffentliche Hand in der Praxis sogar mit dem Auskunftsrecht etwas anzufangen wissen, zeigt *Reichmann*, Das Auskunftsrecht nach dem Datenschutzgesetz 2000 – Eine Fallstudie, ZfV 2004/1529. Bei der von ihm beschriebenen, an der Universität Graz durchgeführten Studie, waren nur 13 Prozent der 39 gestellten Datenschutzanfragen korrekt beantwortet.

22) Siehe zB E DSK 120.819/006 DSK 2003 vom 14.11.2003, *Knyrim*, MR 2004, 51.

23) *Jahnel/Thiele*, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004/55; siehe zu diesem Thema auch *Heil*, Neues Wettbewerbsrecht: Wechselwirkungen zwischen UWG und Datenschutz.

24) Oder auch durch datenschutzrechtlich unzulässige E-Mail-Versendung, *Jaeschke*, „Frühstück ohne SPAM": Fortschritte im Kampf gegen unerwünschte E-Mail-Werbung, ÖJZ 2005, 441; *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in IT.LAW (Hrsg.), e-Mail – elektronische Post im Recht (2003), 89ff; *Knyrim*, nochmals § 107 TKG 2003: Papierwerbung benachteiligt? ecolex 2005, 257.

25) § 1 DSG 2000 ist eine Verfassungsbestimmung, *Drobesch/Grosinger*, Datenschutzgesetz 98.

26) *Dohr/Pollirer/Weiss*, Datenschutzrecht², Anm 4 zu § 4.

27) Art 1 Abs 2 Datenschutzrichtlinie.

28) So muss die Zustimmung zB in Dänemark „explizit" sein, in Italien muss die Zustimmung „schriftlich dokumentiert" werden, in Estland gilt die Zustimmung bis 30 Jahre über den Tod hinaus, in Litauen muss sie bei sensiblen Daten „schriftlich" sein, in der Slowakei muss sie „schriftlich unterfertigt" sein, in England und Irland hingegen gibt es überhaupt keine Definition für den Begriff. Quelle: *Büllesbach*, Referat auf der „East meets West"-Konferenz der Deutschen Gesellschaft für Recht und Informatik, 03.06.2005, Prag.

Gerade in Österreich wurde das Thema Zustimmung eigenwillig streng interpretiert. Ausgehend von einem Rundschreiben des Verfassungsdienstes des Bundeskanzleramtes aus dem Jahre 1978[29]), das sich mit Form und Inhalt einer ausdrücklichen Zustimmungserklärung befasste, hat der OGH in zahlreichen Entscheidungen sehr strenge grundsätzliche Anforderungen an eine Zustimmungserklärung für die Weitergabe von Daten entwickelt.[30]) Dies verlangt, dass die Datenarten, Übermittlungsempfänger und der Zweck der Datenverarbeitung und -übermittlung im Detail zu beschreiben sind.[31])

Diese strengen Anforderungen an die Zustimmungserklärung zu Datenverarbeitungen und -übermittlungen führen in der Praxis zu erheblichen Problemen. So, wenn mit dem Auftraggeber verbundene Unternehmen (Töchter-, Schwester-, Muttergesellschaften) Daten austauschen und die Anwendung der oben genannten Grundsätze dazu führen müsste, dass diese – oft mehrere Dutzend oder sogar Hunderte – in der Zustimmungserklärung alle namentlich genannt werden müssten. In der Praxis versucht man dieses Problem nun verschiedenartig zu lösen, etwa dadurch, dass darauf hingewiesen wird, dass eine Liste der konkreten Empfänger zB im Internet abrufbar ist.

Ein weiteres Problem ist die Zweckdefinition bei Datenübermittlungen, besonders dann nämlich, wenn die Daten für Marketingzwecke weiterverwendet werden sollen, da der Oberste Gerichtshof die pauschale Formulierung „zu Werbezwecken" als Zweckangabe ausdrücklich als zu intransparent beurteilt hat. Dadurch kommt es bei der Formulierung von Zustimmungserklärungen regelmäßig zu einer „Gratwanderung" zwischen einer von den Unternehmen gewünschten, möglichst allgemein formulierten (und damit möglichst viele künftige Eventualitäten abdeckenden) Zweckangabe und dem Risiko, dass diese womöglich wieder zu intransparent ist.

3. Aktuelle Trends

Die oben geschilderten Probleme zeigen, dass sich Unternehmen in den letzten Jahren intensiv mit datenschutzrechtlichen Fragen auseinandergesetzt haben. Ganz allgemein ist in den letzten Jahren eine ständig zunehmende Beschäftigung mit Datenschutzrecht zu beobachten. Dies sowohl in der allgemeinen Öffentlichkeit, ua ausgelöst durch „politische" Vorhaben wie verstärkte Videoüberwachung an öffentlichen Plätzen, Bürgerkarte oder Bildungsdokumentation als auch im unternehmerischen Bereich (hier insbesondere durch die verstärkte An- und Einbindung österreichischer Unternehmen in internationale Konzerne).[32])

In den letzten Jahren lässt sich als „Trend" beobachten, dass Unternehmen Daten ihrer Arbeitnehmer und ihrer Kunden (also Konsumentendaten) verstärkt verarbeiten und intensiver auswerten. Arbeitnehmer werden bei ihrer Tätigkeit stärker elektronisch überwacht als früher[33]) und Arbeitnehmerdaten werden in sehr ausgereiften Human Ressource-Datenverarbeitungssystemen immer mehr aufgearbeitet, um die Arbeitskraft besser einsetzen zu können; selbiges passiert mit den Kundendaten, um einen höheren Mehrwert aus dem Kunden zu generieren und eine größere Kundenbindung zu erreichen (sog Customer Relationship-Management).[34]) Eine noch intensivere Aufarbeitung von Kunden- oder Personaldaten erfolgt beim „Data Mining" und „Data Warehousing".[35])

Als weiterer Trend ist zu beobachten, dass die Datenverarbeitung nicht nur intensiviert wird, sondern bei dieser auch neue Technologien zum Einsatz kommen. Als neue Datenart ist der Standort einer Person entstanden und „Location Based Services"[36]) in den unterschiedlichsten Ausformungen und Technologien (GSM, GPS, UMTS, RFID) verstärken Standortermittlungen und Standortüberwachungen von Produkten als auch direkt oder indirekt[37]) von Menschen. Besonders RFID-Chips mit individuellem Code für jedes Produkt weltweit wird ein baldiger Siegeszug als Nachfolger der heutigen Barcodes prophezeit.[38]) Mit einer anderen

29) Rundschreiben des BKA-VD, 810.008/11a/85 vom 10.8.1988, abgedruckt bei *Dohr/Pollirer/Weiss,* Kommentar zum Datenschutzgesetz (MANZ), Anh IV/2 2.

30) Eine vollständige Darstellung der Judikatur siehe bei *Knyrim,* Datenschutzrecht (MANZ 2003), 178.

31) *Pfarl,* Gefunden! LBS im Mobilfunknetzbereich, ecolex 2005, 569, zeigt das differenzierte Verhältnis von TKG 2003 und DSG 2000 im Hinblick auf Zustimmungserklärungen auf.

32) Das steigende Interesse am Datenschutzrecht spiegelt sich auch in der Statistik der Datenschutzkommission wider, die in den Jahren 2002-2004 beinahe eine Verdopplung der Beschwerden verzeichnet; alleine im ersten Halbjahr 2005 wandten sich fast ebenso viele Bürger an die Datenschutzkommission wegen Rechtsauskünften wie in den beiden Jahren davor (Datenschutzbericht 2005 der Datenschutzkommission, 21 ff).

33) *Kotschy/Reimer,* Die Überwachung der Internetkommunikation am Arbeitsplatz – ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, ZAS 2004, 167; *Brodil,* Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis – Kontrollbefugnisse des Arbeitgebers zwischen Datenschutz und Persönlichkeitsrechten, ZAS 2004, 156.

34) *von Lewinski,* Persönlichkeitsprofile und Datenschutz bei CRM, RDV 2003, 122; *Knyrim,* CRM-Anwender aufgepasst: Datenschutz kann zum Fallstrick werden, Computerwelt 20.5.2005, 14.

35) *Baeriswyl,* Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?, RDV 2000, 6; *Weichert,* Datenschutzrechtliche Anforderungen an Data-Warehouse-Anwendungen bei Finanzdienstleistern.

36) *Fallenböck,* Der Einsatz von Location Base Services – Eine erste Analyse rechtlicher Problemfelder, MR 2002, 182; *Pfarl,* Gefunden! LBS im Mobilfunknetzbereich, ecolex 2005, 569; *Taeger,* Verwertung von Standortdaten durch Private, in Taeger/Wiebe (Hrsg.), Mobilität Telematik Recht (2005), 95.

37) Ein System, das Gabelstapler in einer Lagerhalle zur Optimierung der Lagerhaltung ständig standortüberwacht, kann dazu verwendet werden, die Fahrer bei ihrer Tätigkeit permanent zu überwachen, womit deren Arbeitsleistung durch ein derartiges System indirekt kontrolliert werden kann.

38) Arbeitspapier 105 der Art 29 Datenschutzgruppe über Datenschutzfragen in Zusammenhang mit der RFID-Technik vom 19.1.2005, downloadbar unter http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_de.pdf.

Anwendungsform dieser kontaktlos per Funk auslesbaren Datenchips werden die Österreicher im kommenden Jahr in ihren Reisepässen Bekanntschaft machen, die solche Chips mit biometrischen Daten enthalten werden.[39])

Im unternehmerischen Bereich ist mir aus meiner rechtsberatenden Tätigkeit in den letzten Jahren überdies aufgefallen, dass sich vor allem internationale Unternehmen sehr verstärkt mit Datenschutz beschäftigen, bei denen eigene „Chief Privacy Officers" (CPOs) von höchster Ebene den „Auftrag" an alle Konzerngesellschaften in allen Ländern, in denen sie vertreten sind, erteilen, sich um die Einhaltung des Datenschutzrechts zu sorgen.[40]) Bei österreichischen Klein- und Mittelbetrieben ist eine derartige Zunahme in der Beschäftigung mit Datenschutzrecht nicht so signifikant zu beobachten. Es besteht daher die Gefahr, dass diese gegenüber den großen Konzernen, die Datenschutz immer mehr auch als Marketingargument einsetzen, ins Hintertreffen geraten.

Je intensiver die Beschäftigung internationaler Unternehmen mit Datenschutzrecht ist, desto mehr stehen diese Unternehmen vor dem geschilderten Problem, dass im nur scheinbar durch die Europäische Datenschutzrichtlinie vereinheitlichten Daten-Binnenmarkt tatsächlich 25 im Detail sehr unterschiedliche Datenschutzgesetze bestehen, die von 25 Behörden und von den Gerichten in 25 Mitgliedesländern oft sehr unterschiedlich gehandhabt und unterschiedlich streng ausgelegt werden. Da Datenglobalisierungsprojekte in Konzernen durch diese Situation auf rechtlicher Seite zu „Großprojekten" auswachsen, fordern große Konzerne seit einigen Jahren eine verstärkte Selbstregulierung im Datenschutz.[41]) Ein Ansatz dafür sind die „Codes of Conduct", mit denen der Gedanke eines einheitlichen europäischen Datenschutzrechts verwirklicht werden soll.[42])

4. „Codes of Conduct" als konkrete Entwicklung einer Selbstregulierung

Erster Höhepunkt der Entwicklung zu mehr Selbstregulierung war eine große Datenschutzkonferenz am 30.9. – 1.10.2002 in Brüssel, bei der die Konzerne ihre diesbezügliche Forderung mit großem Nachdruck „offiziell" an die Europäische Kommission herantrugen und argumentierten, dass für sie die verschiedenen lokalen Datenschutznormen und die lokalen Datenschutzgenehmigungsverfahren kaum mehr administrierbar seien.[43]) Die Konzerne boten an, dass sie unternehmensinterne Datenschutzrichtlinien schaffen, die erwähnten „Codes of Conduct" oder „Binding Corporate Rules", auf deutsch „verbindliche unternehmensinterne Datenschutzregelungen", die sie dann konzernweit (europaweit oder sogar weltweit) umsetzen und deren Einhaltung garantieren, dafür im Gegenzug aber Erleichterungen bei den Meldeverfahren (zentralisierte Meldeverfahren) und bei internationalen Datentransfers bekommen. Die ersten bekannten „Codes of Conduct" stammen von Daimler Chrysler und wurden in Deutschland von *Büllesbach*[44]) entwickelt. Mittlerweile gibt es drei Arbeitspapiere[45]) der sog „Art 29-Datenschutzgruppe" zur Frage, wie diese verbindlichen unternehmensinternen Datenschutzregelungen implementiert werden können. Es gibt zwei wesentliche Ansätze: entweder, es werden Verträge mit Konzerngesellschaften untereinander geschlossen[46]) oder der Konzern (die Konzernmutter verbindlich für die übrigen Unternehmensteile) lobt einseitig gegenüber Dritten aus, dass er die „Codes of Conduct" einhalten wird. Die Betroffenen sollen dabei Drittbegünstigte sein. In der EU soll eine Gesellschaft haftbar und klagbar sein, selbst dann, wenn die Verletzung in einer Konzerngesellschaft in einem Drittstaat passiert. Die Arbeitspapiere beschreiben im Detail, wie diese Verfahren ablaufen[47]) und was die Voraussetzungen[48]) dafür sind. Die „Codes of Conduct" sind ein sehr gutes Beispiel, dass eine Selbstregulierung im Datenschutzrecht funktionieren kann, wenn sowohl im Unternehmen aktiv Datenschutzrecht betrieben wird, als auch von staatlicher Seite ein derartiges Verhalten und ein solcher Ansatz gefördert werden.

5. Selbstregulierung als Lösung auch in Österreich

Meines Erachtens ist Selbstregulierung des Datenschutzrechtes auch in Österreich möglich und anzustreben,

---

39) *Knyrim/Haidinger*, RFID-Chips und Datenschutz, RdW 2005, 2.

40) Dies ist ein globaler Trend, der ua daran zu erkennen ist, dass große Konzerne durch ihre „Chief Privacy Officers" nicht nur intern Datenschutzrecht forcieren, sondern auch aktiv an der Weiterentwicklung des Datenschutzrechts auf internationaler Ebene teilnehmen, zB durch Präsentation ihrer Anliegen auf internationalen Kongressen, wie jüngst der im September 2005 in Montreux stattgefundenen 27. Internationalen Konferenz der Datenschutzbehörden. (Eine Nachlese zur Konferenz findet sich unter http://www.edsb.ch.)

41) Tatsächlich gibt es nämlich für Konzerne im Datenschutzrecht überhaupt kein Konzernprivileg und jede Übermittlung im Konzern ist genauso auf ihre rechtliche Zulässigkeit zu prüfen wie eine Übermittlung an außenstehende Dritte.

42) *Weichert,* Regulierte Selbstregulierung – Plädoyer für eine etwas andere Datenschutzaufsicht, in Taeger/Wiebe (Hrsg.), Mobilität, Telematik, Recht (2005), 219 (224).

43) Siehe *Knyrim,* Wenn Telefonlisten im Konzern zum Problem werden, Rechtspanorama, Die Presse, 30.9.2002.

44) „Daimler Chrysler Codes of Conduct", downloadbar unter http://www.daimlerchrysler.de unter „Datenschutz"; *Büllesbach,* Konvergenz durch Standardisierung und Selbstregulierung, in Büllesbach/Dreier (Hrsg.), Konvergenz in Medien und Recht (2002), 213.

45) Arbeitspapiere 107 und 108 der Art. 29 Datenschutzgruppe vom 14.4.2005, downloadbar unter http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_de.pdf, http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_de.pdf und http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_de.pdf.

46) Auch die Aufnahme der Regelungen in die allgemeinen Unternehmensgrundsätze mit entsprechenden Verhaltensregeln, Audits und Sanktionen zu ihrer Durchsetzung ist eine Möglichkeit, siehe Arbeitspapier 108, Pkt 5.6.4.

47) Arbeitspapier 107.

48) Arbeitspapier 74, 108.

wobei aber immer ein sinnvoller und effektiver regulativer Rahmen bestehen muss. Grundvoraussetzung für Selbstregulierung ist, dass zunächst Wissen über Datenschutzrecht besteht oder geschaffen wird und dann von den beteiligten Interessensgruppen der Wille besteht, mit marktwirtschaftlichen Instrumenten gemeinschaftlich aktiv in fairer Form Datenschutzrecht zu betreiben. Dabei darf kein Ungleichgewicht der Kräfte entstehen, da derartige Ungleichgewichte längerfristig auf den zurückfallen, der sie am meisten für sich zunutze machen möchte, seien es die Unternehmen, die staatlichen Aufsichtsorgane, die Betroffenen oder die Daten- und Konsumentenschützer. Auf sachlich-rechtlicher Ebene lassen sich meiner Erfahrung nach mit vertretbaren Mitteln und vertretbarem Aufwand fast immer für alle Beteiligten akzeptable und faire Lösungen finden. Unter der Prämisse eines fairen Interessensausgleichs, die dem Datenschutzgesetz ohnehin immanent ist,[49]) sehe ich keinen Grund, warum eine „regulierte Selbstregulierung" nicht gut funktionieren sollte, in Betracht gezogen allerdings die in den vorigen Punkten ausgeführten Probleme.

Dass Selbstregulierung als Lösungsansatz im Datenschutzrecht sogar ausdrücklich vorgesehen ist, zeigt § 6 Abs 4 DSG 2000. Dieser sieht vor, dass zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach „Treu und Glauben" anzusehen ist, im privaten Bereich gesetzliche Interessensvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten können. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen des Datenschutzgesetzes begutachtet und als gegeben erachtet hat. Die – soweit ersichtlich ersten – Verhaltensregeln nach § 6 Abs 4 DSG 2000 wurden vom Direktmarketingverband Österreich und der Wirtschaftskammer Österreich für die Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen (§ 151 GewO) erstellt und vom Bundeskanzler begutachtet. Adressverlage und Direktmarketingunternehmen, die diese Verhaltensregeln einhalten, können davon ausgehen, dass ihre Datenanwendung eine Datenanwendung nach „Treu und Glauben"[50]) ist. Diese Verhaltensregeln dienen gleichzeitig auch als Interpretationshilfe bei der Auslegung des Datenschutzgesetzes bzw des § 151 GewO, auch wenn im Rahmen der Verhaltensregeln nicht sämtliche offenen Fragen im Hinblick auf Adressverlage und Direktmarketingunternehmen gelöst werden konnten. Dieses erste Selbstregulationsmodell[51]) ist positiv hervorzuheben und zeigt, dass eine Branche, die in den letzten Jahren wiederholt unter der Kritik von Daten- und Konsumentenschützern zu leiden hatte, mit eigener Kraft und gemeinsamem Willen ein Selbstregulierungsmodell schaffen konnte, das nun sogar mittels eines eigenen „Fair Data"-Logos positiv für das Eigenmarketing eingesetzt wird. Es bleibt zu hoffen, dass andere Branchen diesem Beispiel folgen, da derartige Verhaltensregelungen, wie das Beispiel des Direct Marketing Verbandes Österreich zeigt, nicht nur zu einer Selbstregulierung an sich führen, sondern als positive „Nebeneffekte" eine intensive Beschäftigung der beteiligten Unternehmen mit datenschutzrechtlichen Fragen, die Möglichkeit zur Interpretation datenschutzrechtlicher Regelungen – inklusive Begutachtung durch den Bundeskanzler – als auch die Möglichkeit zur anschließenden positiven Eigenwerbung bieten.

49) Siehe zB § 14 – Sicherheit; § 7 Abs 3; § 8 Abs 1 Z 3 DSG 2000.

50) § 6 Abs 1 Z 1 DSG 2000.

51) *Philapitsch*, Selbstregulierung im Datenschutz, MR 2005, 270 (271).