Dr. Rainer Knyrim/Mag. Viktoria Haidinger*

Datenschutzrecht in Österreich aus Sicht der anwaltlichen Praxis

1. Einleitung

Das Jahr 2005 ist ein Zweifach-Jubiläum für den österreichischen Datenschutz: Vor 25 Jahren, am 1.1.1980, trat das erste österreichische Datenschutzgesetz (DSG 1978)[1] in Kraft. Seit fünf Jahren, nämlich seit dem 1.1.2000, gilt das DSG 2000[2] in Österreich. Das Jubiläum als Anlass, werden im Rahmen dieses Berichts die wichtigsten Spezifika des österreichischen Datenschutzrechtes aus der Sicht der anwaltlichen Praxis erörtert, von den Erfahrungen mit den österreichischen Datenschutzbehörden berichtet sowie aktuelle Judikatur und Gesetzgebung erörtert.

2. Kompetenzverteilung, Situation der Datenschutzkommission

Nach dem DSG 1978 war die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automatisationsunterstützten Datenverkehr ausschließlich Bundessache (§ 2 DSG 1978 bzw 2000). Erst mit der Aufnahme von Regelungen über die manuelle Verarbeitung von Daten im DSG 2000 bekamen die Länder Gesetzgebungskompetenz für bestimmte, nach Landesgesetz einzurichtende Dateien, die nach wie vor manuell geführt werden. Darunter fallen beispielsweise manuelle Register im Rahmen des Fischerei- oder Jagdrechts. Die Bedeutung der Landesdatenschutzgesetze ist daher gering und überdies verweisen die meisten ohnehin auf das DSG 2000, sodass auf diese in der Folge nicht weiter eingegangen wird.

Die Zuständigkeit zur Vollziehung teilen sich nach § 1 Abs. 5 und §§ 30–32 DSG 2000 im Wesentlichen die ordentlichen Gerichte und die Datenschutzkommission. Die Datenschutzkommission ist für die Durchsetzung des DSG 2000 gegenüber Auftraggebern des öffentlichen Bereichs sowie für die Durchsetzung des Auskunftsanspruches gegenüber Auftraggebern des privaten Bereiches zuständig. Ferner kommen ihr nach § 30 DSG 2000 ein relativ umfassendes Kontrollrecht gegenüber Auftraggebern und Dienstleistern sowie Genehmigungskompetenzen für den internationalen Datenverkehr zu. Für die restlichen Ansprüche gegenüber Auftraggebern aus dem privaten Bereich, d. h. insbesondere Widerspruchs-, Löschungs- und Richtigstellungsansprüche, sind die ordentlichen Gerichte zur Entscheidung berufen. Die Alleinzuständigkeit für Auskunftsansprüche wurde im DSG 2000 der Datenschutzkommission zugewiesen, weil man sich durch den Entfall des Prozessrisikos eine häufigere Geltendmachung des Auskunftsanspruches erwartete. Durch die Einleitung des Verwaltungsverfahrens entstehen den Betroffenen nämlich ungleich weniger Kosten und Risiken als bei der Durchsetzung im Zivilrechtsweg. Allerdings gehört die Datenschutzkommission zu jenen Datenschutzstellen in Europa, die personell am schlechtesten ausgestattet sind, was sich auf die Verfahrensdauer erheblich auswirkt. Beschwerdeverfahren, Genehmigungen internationaler Datentransfers sowie Erledigung von Meldung beim Datenverarbeitungsregister können sich über viele Monate hinziehen. Obwohl die wenigen Mitarbeiter der

* Dr. Rainer Knyrim ist Rechtsanwalt und Partner, Mag. Viktoria Haidinger, LL.M. ist Rechtsanwaltsanwärterin bei Preslmayr Rechtsanwälte, Wien. Korrespondenzadresse: A-1010 Wien, Dr. Karl Lueger-Ring 12, knyrim@preslmayr.at.

1 DSG 1978, BGBl 565/1979.

2 BGBl I 165/1999.

Datenschutzkommission sehr bemüht und entgegenkommend sind[3], können fehlende Mittel durch noch so viel Engagement nicht völlig wettgemacht werden. Die Datenschutzkommission selbst spricht in ihrem im August 2005 veröffentlichten Datenschutzbericht 2005 eine sehr deutliche Sprache über ihre Situation, die sie als „unhaltbar" bezeichnet, und wo von „organisatorischen Wirren" berichtet wird. In den Jahren 2002 bis 2003 seien durchschnittlich nur drei Mitarbeiter für die Bearbeitung von Beschwerdeverfahren zur Verfügung gestanden und die Gesamtsituation sei mit 1. Mai 2005 durch Schaffung einer Planstelle für die Betreuung der supra- und internationalen Agenden der Datenschutzkommission nur geringfügig verbessert worden. 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 (Deutschland war in dieser Statistik nicht enthalten)[4].

Judikatur zum Datenschutzgesetz des in Zivilsachen in letzter Instanz zuständigen österreichischen Obersten Gerichtshofs (OGH) gibt es wenig. Einige Schwerpunkte sind auszumachen: Vor allem durch Verbandsklagen des Vereins für Konsumenteninformation hat der OGH eine äußerst strenge Judikatur zu den Anforderungen an Zustimmungserklärungen entwickelt. Im Zusammenhang mit dem Gesetz gegen den unlauteren Wettbewerb (UWG) hat sich der OGH wiederholt mit dem Datenschutzgesetz beschäftigt und in Arbeitsrechtsachen- meist veranlasst durch die Belegschaftsvertretung- gibt es ebenfalls einige Entscheidungen des Höchstgerichtes.

Trotz der oben geschilderten Situation soll nicht der Eindruck erweckt werden, dass Datenschutzrecht in Österreich kein Thema sei. Im Gegenteil ist in den letzten Jahren eine ständig zunehmende Beschäftigung mit Datenschutzrecht zu beobachten. Dies sowohl in der allgemeinen Öffentlichkeit (insbesondere ausgelöst durch „politische" Vorhaben wie verstärkter Videoüberwachung an öffentlichen Plätzen oder der elektronischen Gesundheitskarte (e-Card) des Hauptverbandes der Österreichischen Sozialversicherungen) als auch im unternehmerischen Bereich (hier insbesondere durch die verstärkte An- und Einbindung österreichischer Unternehmen in internationale Konzerne)[5]. Auf die die allgemeine Öffentlichkeit betreffenden „politischen" Datenschutzrechtsthemen wird in diesem Bericht nicht weiter eingegangen, sondern es werden die für in Österreich tätigen Unternehmen wichtigsten Punkte aus dem Datenschutzrecht nachstehend näher beleuchtet.

3. Die Meldung von Datenanwendungen und -übermittlungen und Genehmigung internationaler Datentransfers

Zur Sicherung der Publizität von Datenverarbeitungen bedient sich der österreichische Gesetzgeber im DSG 2000 wie schon im DSG 1978 in erster Linie des Instruments eines Registers der Datenanwendungen. Da im österreichischen DSG die Funktion eines internen betrieblichen Datenschutzbeauftragten nicht vorgesehen ist, besteht grundsätzlich eine direkte Meldepflicht der Datenverarbeitungen beim Datenverarbeitungsregister für jede Datenanwendung. Von dieser Meldepflicht gibt es allerdings eine Reihe von Ausnahmen durch so genannte Standardanwendungen, die durch die Standard- und Musterverordnung[6] festgelegt wurden und die typische Standardfälle von Datenverarbeitungen von der Meldung freistellt. Für den privaten Bereich sind insbesondere die Datenanwendungen SA001 Rechnungswesen und Logistik, SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse sowie die SA022 Kundenbetreuung und Marketing für eigene Zwecke relevant. Bei diesen ist genau geregelt, welchen Zweck die jeweilige Datenanwendung hat, welche Datenarten verarbeitet werden dürfen sowie an welche Empfängerkreise die Daten übermittelt werden dürfen, ohne eine weitere Meldepflicht auszulösen. Für die Praxis bedeutet dies, dass die im Betrieb bestehenden Datenanwendungen und -übermittlungen analysiert und mit den Standardanwendungen verglichen werden müssen. Verarbeitet der Betrieb mehr Datenarten oder übermittelt sie an andere Empfänger als in den Standardanwendungen angeführt, besteht eine Meldepflicht, sonst nicht. Festzuhalten ist, dass die formelle Meldepflicht nichts mit der materiellen Zulässigkeit der Datenverwendung im konkreten Einzelfall zu tun hat.

Einige typische Praxisfälle bei diesem Meldesystem seien hervorgehoben: Während die Kunden- und Lieferantendatenverarbeitung nach der SA001[7] eine Übermittlung zumindest von Großkundendaten an die Konzernleitung des Auftraggebers vorsieht, muss die Übermittlung von Arbeitnehmerdaten z. B. von Österreich an die deutsche Schwester- oder Muttergesellschaft gemeldet werden, da Konzerngesellschaften in der einschlägigen Standardanwendung SA002 als Empfänger nicht vorgesehen sind. Dies ist gerade aber einer der häufigsten Fälle, da Niederlassungen internationaler Konzerne in Österreich oft so klein sind, dass die Personalverwaltung beispielsweise bei der Mutter- oder auch der Schwestergesellschaft in Deutschland angesiedelt ist. Sowohl Datenüberlassungen an Dienstleister als auch Datenübermittlungen an Verarbeiter außerhalb der EU (z. B. in die USA) sind unabhängig von ihrer Meldepflicht zusätzlich vorab genehmigungspflichtig bei der Datenschutzkommission, wobei die Hauptschwierigkeit bei solchen Genehmigungen im tatsächlichen Bereich liegt. Häufig ist es nämlich problematisch, in der von der Datenschutzkommission geforderten Konkretheit festzustellen, welche Daten zu welchen Zwecken überhaupt übermittelt werden sollen. Einer Übermittlung von Personaldaten steht die Datenschutzkommission meist mit besonderem Argwohn gegenüber, denn ihr ist die Notwendigkeit der selbstständigen Verarbeitung von Daten durch die Konzernmutter nicht leicht erklärbar. Ihr ist z. B. ohne eingehende Begründungen nicht ersichtlich, warum die Konzernmutter (etwa in den USA) ohne weiteres einsehen können soll, wer bei der österreichischen Tochtergesellschaft wie oft krank ist oder wo die Sekretärin X privat wohnt, was mangels strenger Zugriffsbeschrän-

3 Die Verfasser können aus eigener Erfahrung sogar über am Sonntag (!) von Mitarbeitern der Datenschutzkommission versandte E-Mails berichten.

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

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

6 Derzeit in Kraft ist die Standard- und Musterverordnung 2004 (StMV 2004), BGBl II 312/2004.

7 Von der offiziellen Bezeichnung „Rechnungswesen" sollte man sich nicht verwirren lassen.

kungen oft die praktische Konsequenz einer konzernweit zentralisierten HR-Datenverwaltung ist. Die Überlassung und Übermittlung von Kunden- und Lieferantendaten ist im Hinblick auf den Erlaubnistatbestand „Vertragserfüllung" etwas leichter zu argumentieren, was jedoch nicht heißt, dass die Verfahren besonders einfach sind. Der Bedarf nach diesen Datentransfers ist insbesondere durch die Nutzung umfassender und zentralisierter (Konzern-) Datenverarbeitungssysteme in Österreich in den letzten Jahren stark gestiegen.

Entsprechend den Vorgaben der Richtlinie besteht für Datenanwendungen, die sensible oder strafrechtlich relevante Daten verarbeiten oder die in Form eines Informationsverbundsystems geführt werden, eine Vorabgenehmigungspflicht bei der Datenschutzkommission.

Nach § 20 Abs. 1 DSG 2000 können die Datenschutzkommission und das Datenverarbeitungsregister, wenn sie zur Auffassung gelangen, dass eine Meldung mangelhaft ist, dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer Frist auftragen. Dies führt in der Praxis leider dazu, dass vor allem das Datenverarbeitungsregister diese Frist zunächst fast „ausreizt" und knapp vor Ablauf einen (oft sehr formalistischen) Verbesserungsauftrag erteilt, womit sie aus dieser zweimonatigen Frist herausfällt und nur noch der allgemeinen maximalen Entscheidungsfrist von sechs Monaten nach § 73 Abs. 1 Allgemeines Verwaltungsverfahrensgesetz (AVG) unterliegt[8]. Bei Verletzung dieser Pflicht stünde dem Auftraggeber der Rechtsbehelf der Säumnisbeschwerde nach Art. 130 Abs. 1 lit. b Bundes-Verfassungsgesetz (BVG) an den Verwaltungsgerichtshof offen, der jedoch angesichts der notorischen Überlastung dieses Höchstgerichtes gut zu überlegen ist.

In Verfahren, besonders bei dringlichen Genehmigungsverfahren, empfiehlt sich vor allem ein regelmäßiger persönlicher Kontakt zu den zuständigen Sachbearbeitern (telefonisch, E-Mail, persönliche Vorsprache), um allfällige Probleme möglichst rasch gemeinsam lösen zu können.

4. Datenschutzrechtliche Zustimmung

Ausgehend von einem Rundschreiben des Verfassungsdienstes des Bundeskanzleramtes aus dem Jahre 1978[9], das sich mit Form und Inhalt einer ausdrücklichen Zustimmungserklärung befasste, hat der OGH in zahlreichen Entscheidungen folgende grundsätzliche Anforderungen an eine Zustimmungserklärung für die Weitergabe von Daten entwickelt[10]:

1. Die Datenarten, Übermittlungsempfänger und der Zweck der Datenverarbeitung und -übermittlung sind genau zu beschreiben.
2. Ein ausdrücklicher Hinweis auf den jederzeit möglichen schriftlichen Widerruf ist aufzunehmen.
3. Die Zustimmungsklausel ist im Text hervorzuheben.
4. Erfolgt die Datenübermittlung in Länder ohne angemessenes Datenschutzniveau, ist darauf entsprechend hinzuweisen.

Im Jahre 1999 erachtete der OGH in seiner „Friends of Merkur-Entscheidung"[11] folgende Zustimmungsklausel für nichtig, weil sie dem Transparenzgebot des § 6 Abs. 2 öKSchG widersprach. Es war laut OGH nicht klar, an welche Unternehmen (die namentlich zu nennen gewesen wären) im X-Konzern die Daten gingen:

„Ich bin ausdrücklich damit einverstanden, dass meine oben genannten persönlichen Daten EDV-unterstützt verarbeitet und zum Zwecke der Konsumenteninformation sowie allfälliger Werbemaßnahmen an andere Unternehmen des X-Konzerns weitergegeben werden."[12]

In zwei Entscheidungen zu den AGB der Banken[13] erklärte der OGH eine Reihe von Klauseln für nichtig, mit denen der Betroffene zu pauschal in die Weitergabe seiner Daten an Gemeinschaftseinrichtungen, die „Kleinkreditevidenz" und die „Warnliste" beim Kreditschutzverband von 1870 und andere Interessenten, unter Entbindung des Bankgeheimnisses, einwilligte.

Zwischendurch traf es auch einen Mobilfunkbetreiber, dessen folgende Klausel gleichfalls für nichtig erkannt wurde[14]:

„Zu Werbezwecken erfolgt auch ein Datenaustausch mit Konzernunternehmen und eine Datenübermittlung auch an andere Dritte, sofern der Teilnehmer dem nicht bei Teilnahmebeginn oder zu einem späteren Zeitpunkt widerspricht."

Zu intransparent waren dem OGH hier die „Werbezwecke" und wieder die Übermittlungsempfänger.

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 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 z. B. im Internet abrufbar ist und sich diese ändern kann.

Ein weiteres Problem ist die Zweckdefinition der Datenübermittlung und zwar besonders, wenn die Daten für Marketingzwecke weiterverwendet werden sollen, da der Oberste Gerichtshof die pauschale Formulierung „zu Werbezwecken" als Zweckangabe, wie oben beschrieben, ausdrücklich als intransparent beurteilt hat. Dadurch kommt es in der Praxis 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 eine solche womöglich wieder zu intransparent ist.

8 Diese läuft ab Einlangen des verfahrenseinleitenden Schriftsatzes.

9 Rundschreiben des BKA-VD, 810.008/1-1a/85 vom 10.08.1988, abgedruckt bei Dohr/Pollirer/Weiss, Kommentar zum Datenschutzgesetz (MANZ), Anh. IV/2 2.

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

11 OGH 27.01.1999, 7 Ob 170/98w = ecolex 1999, 182 = RdW 1999, 458. Ein Großteil der hier zitierten Entscheidungen finden sich im RIS.

12 Vgl auch die am selben Tag zu einem ähnlich gelagerten Fall ergangene Entscheidung des OGH 7 Ob 326/98m = RdW 1999, 457.

13 OGH 22.3.2001, 4 Ob 28/01y, ecolex 2001, 147 (mit Glosse von Rabel) – AGB der Banken I und OGH 19.11.2002, 4 Ob 179/02 f. = ÖBA 2003, 41 – AGB der Banken II.

14 OGH 13.09.2001, 6 Ob 16/01y = JBl 2002, 178 = ecolex 2002, 86 (mit Glosse von Leitner) – Mobilpoints.

5. Datenschutzrecht und Wettbewerbsrecht

Im Bereich des öUWG hat es gleichfalls schon eine Reihe von Entscheidungen mit datenschutzrechtlich relevanten Aspekten gegeben. Erstmalig im Jahr 1992 stellte der OGH fest[15], dass die Auswertung der Girokonten auf Einzahlungen in Bausparverträge bei anderen Banken (Fremdbausparer), um diesen Kunden Werbematerial über Bausparverträge zusenden zu können, sowohl eine Verletzung des Bankgeheimnisses als auch des DSG darstelle, und dieser Rechtsbruch dem beklagten Unternehmen einen unlauteren Vorteil ermögliche.

Interessant war das jüngste Urteil des OGH[16] aus dem Jahr 2004. Im Rahmen eines Verfahrens zur Erlassung einer einstweiligen Verfügung nach UWG stand aufgrund von gleichlautenden Tippfehlern in Kundennamen fest, dass offensichtlich Kundenlisten an einen Konkurrenten gelangt waren. Da der Konkurrent nicht glaubwürdig nachweisen konnte, wie diese Kundendaten in seinen Besitz gelangt waren, vermutete der OGH einen unredlichen Erwerb dieser Daten und entschied zu Gunsten der gefährdeten Partei, die einen Wettbewerbsnachteil wegen des Anschreibens ihrer Kunden argumentiert hatte.

Kurz zuvor erging eine Entscheidung des OGH[17], die in der Lehre auf heftige Kritik wegen der Fehlinterpretation datenschutzrechtlicher Grundsätze stieß[18]. Der OGH erachtete es in dieser für zulässig, dass ein ehemaliger Mitarbeiter Kunden- und Lieferantendaten sowie Kalkulationsunterlagen seines früheren Arbeitgebers für eigene Geschäftszwecke verwendete, weil der OGH dem ehemaligen Arbeitgeber jegliche Eigenschaft bzw. Rechte als Betroffener mit dem (unzutreffenden) Argument, es handle sich bloß um eigene Daten des Unternehmens, die nicht unter den Schutz des DSG fallen, absprach. Man kann nur hoffen, dass diese Entscheidung ein Einzelfall bleiben wird.

6. Datenschutzrecht und Arbeitsrecht

Mit einer Entscheidung im Jahr 2002[19] urteilte der OGH, dass eine Anlage, die bei Privatgesprächen (jedenfalls Teile) der Rufnummern unterdrückt, dienstlich angewählte Rufnummern aber zur Gänze registriert und für einen kurzen Zeitpunkt „bloß aufbewahrt", der zwingenden Mitbestimmung des Betriebsrates nach § 96 Abs. 1 Z 3 Arbeitsverfassungsgesetz (ArbVG) unterliegt und nur unter besonderen Voraussetzungen in den Geltungsbereich des § 96a ArbVG (ersetzbare Zustimmung des Betriebsrates) wechselt. Er wich damit von der ständigen Judikatur des Verwaltungsgerichtshofes, der lange Zeit für diese Angelegenheiten zuständig gewesen war, ab[20]. Die Entscheidung stieß in der Lehre ebenfalls auf erhebliche Kritik[21], nicht nur weil das Höchstgericht bei seiner Entscheidung Informationspflichten nach dem DSG 2000 und dem § 91 Abs. 2 ArbVG nicht einmal erwähnte, sondern auch weil offenbar unerheblich war, dass im konkreten Fall die bloß registrierten Rufnummern gar nicht ausgewertet worden waren.

Jüngst hatte sich das Oberlandesgericht Wien mit der Frage zu beschäftigen, ob der Betriebsrat für einen Antrag auf einstweilige Verfügung nach dem DSG 2000 legitimiert ist[22]. Wieder ging es um die Durchsetzung des Mitbestimmungsrechts nach § 96a Abs. 1 Z 1 ArbVG. Das OLG Wien sprach dem Betriebsrat das Recht auf eine einstweilige Verfügung nach § 32 Abs. 3 DSG 2000 unter Hinweis auf seine mangelnde Rechtsfähigkeit, seine mangelnde Legitimation für die Durchsetzung privatrechtlicher Ansprüche der Belegschaft und seine mangelnde Betroffenenstellung ab.

Die Datenschutzkommission gab in einer etwa zur selben Zeit ergangenen Entscheidung Ende des Jahres 2004[23] der Beschwerde eines Beamten des Finanzministeriums statt, die sich gegen die Protokollierung jener Zeitpunkte, an denen die Arbeitnehmer den Beginn und das Ende ihrer Arbeitszeit selbstständig in die computerisierte Zeitkarte eintragen, richtete. Grundsätzlich gestand die Datenschutzkommission einem Arbeitgeber ein berechtigtes Interesse an der Kontrolle der Einhaltung der Arbeitszeit durch die Arbeitnehmer zu, hielt es aber für einen unzulässigen Eingriff in das Grundrecht auf Geheimhaltung personenbezogener Daten, dass auch der Zeitpunkt der Eintragung mitprotokolliert wurde.

7. Aktuelle Gesetzgebung

Im DSG 2000 selbst hat sich in den letzten 5 Jahren – mit Ausnahme eines § 48a DSG 2000, der infolge der Tsunami-Katastrophe im Dezember 2004 hinsichtlich der Verwendung von Daten im Katastrophenfall eingefügt wurde[24] – inhaltlich nichts geändert.

Die Standardanwendungen der Standard- und Musterverordnung werden hingegen laufend ergänzt und vermehrt.

Abzuwarten bleiben die Auswirkungen des am 5. Juli 2005 von der EU-Kommission gegen die Republik Österreich eingeleiteten Vertragsverletzungsverfahrens wegen mangelhafter Umsetzung der Datenschutzrichtlinie (laut EU-Kommission ist die „völlige Unabhängigkeit" der Datenschutzkommission nicht gewährleistet)[25].

Datenschutzrechtliche Sonderbestimmungen finden sich in Österreich in einer Reihe von Materiegesetzen, von denen hier das Telekommunikationsgesetz 2003[26], das Strafgesetzbuch[27], das Sicherheitspolizeigesetz[28], das E-Governement-Gesetz[29] oder die kürzlich in der Zivilprozessordnung und dem Gerichtsorganisationsgesetz eingefügten datenschutzrechtlichen Bestimmungen im Hinblick auf Akteneinsicht und Auskunftsrecht erwähnt seien[30].

---

15 OGH 25.02.1992, 4 Ob 114/91 – Bausparerwerbung.
16 OGH 6.07.2004, 4 Ob 107/04b – Kundenliste.
17 OGH 4.05.2004, 4 Ob 50/04p – Eigene Daten.
18 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, E 5 zu § 4.
19 OGH 13.06.2002, 8 Ob A 288/01p = ZAS 2004, 40 = WBl 2002, 518 (mit Anm. Thiele); dazu auch Brodil, ZAS 2004, 17.
20 Vgl. VwGH 11.11.1987, 87/01/003; VwGH 9.11.1988, 86/01/0069; EA Linz ZAS 1986, 171.
21 Vgl. nur Brodil, Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis, ZAS 2004, 156.
22 OLG Wien 29.11.2004, 10 Ra 164/04t.
23 DSK 16.11.2004, K 120.951/0009-DSK/2004.
24 BGBl I 13/2005.
25 Der Standard, 11. August 2005.
26 BGBl I 2003/70.
27 BGBl 1974/16, insbesondere § 126a Datenbeschädigung und § 148a betrügerischer Datenverarbeitungsmissbrauch sowie die Computerstraftatbestände §§ 118a ff.
28 BGBl 1991/566.
29 BGBl I 2004/10.
30 § 219 ZPO, RGBl 1895/113 i.d.F. BGBl I 2004/128, §§ 83 ff Gerichtsorganisationsgesetz, RGBl 1896/217 i.d.F. BGBl I 2004/128.

Erwähnt werden soll auch, dass viele Sondergesetze ausdrücklich darauf verweisen, dass die Bestimmungen des Datenschutzgesetzes unberührt bleiben, so z. B. § 2 E-Commerce-Gesetz[31] oder das Informationsweiterverwendungsgesetz, mit dem die PSI-Richtlinie in Österreich umgesetzt werden soll[32].

8. Weiterführende Informationen

Es gibt wenig Literatur zum österreichischen DSG 2000. Das umfangreichste Werk ist der als Loseblattsammlung herausgegebene Kommentar von Dohr/Pollirer/Weiss (erschienen im MANZ Verlag). Für den alltäglichen Gebrauch durchaus hilfreich sind auch der Kurzkommentar von Drobesch/Grosinger (Verlag Juridica, 2000), ebenso jener von Drobesch/Rosenmayr-Klemenz (Wirtschaftskammer Österreich, 2000). Ferner gibt es zwei weitere Werke, die das DSG 2000 kurz im Überblick erklären und zwar von Mayer-Schönberger/Brandl, DSG 2000 (Verlag Linde, 1999) und Jahnel, Datenschutzrecht in der Praxis (dbv-Verlag, 2004).

Das erste und bisher umfangreichste „Praxishandbuch Datenschutzrecht" erschien 2003 im MANZ Verlag von Knyrim.

Datenschutzrelevante Themen werden sporadisch vor allem in den Fachzeitschriften ecolex, Medien und Recht und Recht der Wirtschaft behandelt[33]; Fachartikel zum Thema Arbeitnehmerdatenschutz auch in der Fachzeitschrift ZAS. Eine Fachzeitschrift, die sich ausschließlich mit Datenschutzrecht und -sicherheit beschäftigt, existiert in Österreich nicht.

Knappe Informationen zum nationalen und internationalen Datenschutzrecht, Formulare und Merkblätter sowie eine zweisprachige (deutsch/englisch) Version des DSG 2000 enthält die Webseite der Datenschutzkommission, www.dsk.gv.at. Die meisten Entscheidungen der Datenschutzkommission sind im Rechtsinformationssystem des Bundes (RIS) kostenlos abrufbar (www.ris.bka.gv.at). Ebendort kann man auch die meisten Entscheidungen des Obersten Gerichtshofes und der Gerichtshöfe des öffentlichen Rechts (Verfassungs- und Verwaltungsgerichtshof) abrufen.

---

31 BGBl I 2001/152.

32 Zur Umsetzung der PSI-Richtlinie (RL 2003/98/EG vom 17.11.2003 über die Weiterverwendung von Informationen des öffentlichen Sektors) gibt es derzeit erst die Regierungsvorlage für ein Bundes-Informationsweiterverwendungsgesetz (1026 der Beilagen zu den stenografischen Protokollen des Nationalrates XXII GP) sowie die Entwürfe einiger Landesgesetze, siehe dazu Knyrim, PSI-Richtlinie und Informationsweiterverwendungsgesetz: Der neue Rechts- und Wirtschaftsbereich, Österreichische Zeitschrift für Vermessung und Geoinformation, 1/2005, 17 sowie Knyrim, PSI-Richtlinie und Informationsweiterverwendungsgesetz: Ein neuer Rechtsbereich, Österreichische Gemeindezeitung 8/2005, 36.

33 Diese sind online (kostenpflichtig) teils über www.rdb.at und teils über www.lexisnexis.at abzurufen. Sämtliche von den Autoren dieses Artikels zum Datenschutzrecht abgefassten Fachzeitschriftenbeiträge sind (kostenlos) unter www.preslmayr.at (unter Partner – Knyrim) abrufbar.