Stellungnahme der ARGE DATEN zum

Datenschutzgesetz 1998

(Entwurf des Bundeskanzleramtes in der Fassung des Begutachtungsverfahrens)

Grundsätzliches

Bis zum 24. Oktober 1998 muß die EU-Datenschutzrichtlinie in österreichisches Recht umgesetzt werden. Der vom Bundeskanzleramt vorgelegte Entwurf kann diesem Anspruch trotz mancher Verbesserungen gegenüber früheren Entwürfen noch nicht gerecht werden:

- Der Entwurf bleibt zu stark an den **veralteten begrifflichen Konzepten** des DSG hängen und läßt neue Regelungsansätze wie das Recht auf informationelle Selbstbestimmung völlig außer acht.

- In einer Reihe von Punkten **widerspricht der Entwurf der EU-Richtlinie**, die durch ihn eigentlich umgesetzt werden sollten: Dies betrifft insbesondere das **Verarbeitungsverbot für sensible Daten**, die Anforderungen an die **Qualität der Daten**, die von der Richtlinie neu geschaffene **Informationspflicht** und das **Widerspruchsrecht gegen Direktwerbung**.

- Einige wesentliche Punkte wie insbesondere die kompetenzrechtliche Grundlage fehlen noch völlig.

Die ARGE DATEN fordert daher eine gründliche Überarbeitung des Entwurfs. Von zentraler Bedeutung sind dabei die folgenden Punkte:

1. Das Grundrecht auf Datenschutz soll in Richtung eines **Grundrechtes auf informationelle Selbstbestimmung** neu formuliert werden.
   Dieses informationelle Selbstbestimmungsrecht entspricht auch der internationalen Datenschutzdiskussion. Es wird damit die Eigenverantwortung der Betroffenen bezüglich Ihrer Daten stärker betont und der Gesetzgeber bringt klar und unmißverständlich zum Ausdruck, daß er einen ganzheitlichen und umfassenden Datenschutz für die Bürger wünscht.

2. Die Richtlinie schreibt für **sensible Daten ein generelles Verarbeitungsverbot** mit wenigen, genau aufgezählten Ausnahmen vor. Der Entwurf stellt dieses generelle

Verarbeitungsverbot durch die Generalklausel „Sensible Daten *dürfen jedenfalls* verwendet werden, wenn ...“ (§ 41) auf den Kopf. **Der Entwurf widerspricht in diesem Punkt klar der Richtlinie.**

3. Der vorgeschlagene § 3 enthält ein noch schlimmeres Begriffswirrwarr als der bestehende Gesetzestext. Die Begriffe stellen auf veraltete technische Konzeptionen der 70er-Jahre ab und müssen – schon allein aus Gründen der sorgfältigen Umsetzung der Richtlinie – durch die moderneren **Begriffskonzepte der Richtlinie** ersetzt werden.
   Das Uraltkonzept des DSG wurde im Zuge der Beratung der EU-Richtlinie schon im Jahre 1992 (!) als veraltet verworfen. Bis zu diesem Zeitpunkt sah die ursprünliche EU-Richtlinie - analog dem alten DSG - unterschiedliche Regelungen für Ermittlung, Auswertung und Weitergabe von Daten vor. Seit dem 15.10.1992 (!) enthalten alle EU-Konzepte (inkl. der verabschiedeten Richtlinie) das **neue und der modernen Datenverarbeitung angepaßte Konzept, alle Datenverarbeitungschrite gemeinsam und gleich zu regeln.**
   Der vorliegende Entwurf ignoriert somit die internationale Datenschutz- und Datenverarbeitunsgentwicklung von mehr als 6 Jahren!

4. Ein wesentlicher Fortschritt der Richtlinie gegenüber dem geltenden DSG besteht darin, daß die Richtlinie eine Reihe von Anforderungen für die **Qualität der verarbeiteten Daten** aufstellt – insbesondere müssen Daten einer strengen Zweckbindung entsprechen und wenn nötig, auf den neuesten Stand gebracht werden. **Der Entwurf übernimmt diese Bestimmung zwar (§ 5), degradiert sie aber ganz bewußt zu einer bloßen Soll-Bestimmung und unterläuft damit ein grundlegendes Konzept der Richtlinie.**

5. Die **Datenschutzinstitutionen bedürfen einer grundlegenden Reform**, um die Durchsetzung der Datenschutzrechte zu gewährleisten. Insbesondere fehlt in Österreich eine Institution, die von Amts wegen Datenschutzanliegen aufgreift und advokative Funktionen wahrnimmt. Diese Institution soll in Form eines Bundesdatenschutzbeauftragten eingerichtet werden. Die Kompetenzen sollen klarer in Entscheidungskompetenzen (DSK) und advokative Kompetenzen (Bundesdatenschutzbeauftragter) getrennt werden.

6. Nicht bewährt hat sich bisher die **Rechtsdurchsetzung Betroffener gegenüber privater Datenverarbeiter**. Die

bisherige Lösung, Klagen vor dem jeweiligen Landesgericht einzubringen, bedeutete Anwaltszwang, hohes Prozeßrisiko und angesichts der geringen Erfahrungswerte und vergleichbarer Prozesse ein ungeheures Prozeßrisiko. Sollte dann - wie in der Vergangenheit geschehen - aus formalen Gründen eine Klage abgewiesen werden, müssen eigene und fremde Anwaltskosten bezahlt werden. Selbst bei einfachsten Verfahren ergaben sich rasch Kosten von 30.000.- und mehr. Dies führte dazu, daß es im privaten Bereich praktisch kaum Entscheidungen gab. Dies ist rechtspolitisch unbefriedigend, da gesetzliche Übertretungen nicht geahndet werden.
Es kann nun verführerisch sein, wie im vorliegenden Entwurf vorgeschlagen, Teile der Rechtsdurchsetzung von den Gerichten zu einer Verwaltungsbehörde, der Datenschutzkommisson zu verlegen. Dies widerspricht jedoch den grundsätzlich unterschiedlichen Rechtsdurchsetzungswegen im öffentlichen und im privaten Bereich.
Die ARGE DATEN hat daher einen wesentlich klareren und der österreichischen Rechtsordnung besser angepaßten Vorschlag erarbeitet.
Die Trennung der Behördenzuständigkeit zwischen DSK (öffentlicher Bereich) und Zivilgerichten (privater Bereich) soll grundsätzlich beibehalten werden. Die Rechtsdurchsetzung im privaten Bereich soll jedoch durch die Möglichkeit von Außerstreitverfahren wesentlich erleichtert werden.
Dieses Konzept sieht die Zuständigkeit der Bezirksgerichte vor. Dies bedeutet niedriger, fester Streitwert, kein Anwaltszwang, kein Kostenersatz der Vertretungskosten der gegnerischen Partei. Mit diesem Konzept können Klagen, ähnlich wie vor der Datenschutzkommission, relativ formlos und kostengünstig abgewickelt werden.
Zusätzlich sollen Vertretungs- und Klagemöglichkeiten durch Datenschutzorganisationen und sonstige Konsumenten/Betroffenen-Organisationen geschaffen werden (denkbar wären Gewerkschaft, Arbeiterkammer, Verein für Konsumentenschutz).
Diese Lösung entspricht auch der grundsätzlichen Entwicklung zum "schlanken" Staat. Es erscheint in der heutigen Zeit unsinnig, einer Behörde zusätzliche Aufgaben, noch dazu verfassungsrechtlich problematische Aufgaben, aufzubürden.

7. Die EU-Richtlinie zielt ausdrücklich nur auf den Schutz natürlicher Personen ab. Sinn dieser Beschränkung ist, daß viele informationsrechtliche Tatbestände nur auf natürliche Personen zutreffen können. So können etwa nur

natürliche Personen Träger besonders sensibler Daten, wie Daten zur Gesundheit oder zur weltanschaulichen Überzeugung sein.
Die im vorliegenden Entwurf weiterhin bestehende formale Gleichsetzung der Daten juristischer und natürlicher Personen behindert im Ergebnis die Umsetzung der Richtlinie und führt (siehe oben) zu einer Reihe von Fehlern.
Es wird daher vorgeschlagen, den Schutz juristischer Personen aus dem Entwurf herauszunehmen.
Für juristische Personen ergibt sich daraus faktisch keine Schlechterstellung. Einerseits sind Ihre Daten weiterhin nach den Bestimmungen zum Betriebsgeheimnis (Strafgesetzbuch) geschützt, andererseits gelten ja die Regelungen des Datenschutzes weiterhin, sobald es sich um Informationen über Vertreter, Inhaber usw. von juristischen Personen handelt.

A. Allgemeiner Teil

1. Grundrecht auf informationelle Selbstbestimmung

a) Auch die neue Formulierung des Grundrechtes konzipiert dieses als Abwehrrecht. Der Wille oder hypothetische Wille des Betroffenen spielt in § 1 DSG keine Rolle. Vielmehr wird anhand objektiver Kriterien überprüft, ob ein Eingriff in das Grundrecht zulässig ist. Moderner ist die Konzeption des „Grundrechts auf informationelle Selbstbestimmung“, wie es das deutsche Bundesverfassungsgericht aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG abgeleitet hat: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, *grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*.“ (BVerfGE 65, 1 = EuGRZ 1983, 577). Diesen Gedanken sollte auch das österreichische Grundrecht auf Datenschutz aufgreifen.

b) Es wird vorgeschlagen, nur natürliche Personen in den Schutzbereich des Grundrechtes aufzunehmen, da juristische Personen kein vergleichbar schützenswertes Privat- und Familienleben haben.

Der Schutz juristischer Person hat in der Vergangenheit z. B. nach Ansicht mancher Autoren auch umweltrelevante Daten umfaßt (vgl. dazu die Kontroverse zwischen Duschanek und Trettenbein in RdW 1988, 310; 1989, 325; 1990, 75f), was im Ergebnis Datenschutz für Umweltverschmutzer bedeuten würde.

Ein Textvorschlag ist unten im besonderen Teil abgedruckt.

2. Einbeziehung aller Verarbeitungsarten

Ein zentraler Unterschied zwischen der Richtlinie und dem derzeitigen DSG besteht darin, daß die Richtlinie nicht zwischen automatisierter und manueller Verarbeitung unterscheidet. Entscheidend ist nach der Richtlinie vielmehr, ob eine Sammlung von Daten nach bestimmten personenbezogenen Kriterien strukturiert ist.

Der Anwendungsbereich der Richtlinie erstreckt sich gemäß ihrem Art. 3 Abs. 1 auf die „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen“. Dabei ist „Datei“ in Art. 2 lit. c) definiert als „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind“.

Demgegenüber lautet der zentrale Begriff des Entwurfs nach wie vor „Datenverarbeitung“ und stellt auf automationsunterstützte Verarbeitung ab (§ 3 Z 7). Nur als Variante in eckigen Klammern werden manuelle Verarbeitungen angesprochen: „[als Datenverarbeitung gilt weiters auch jede nicht automationsunterstützt geführte Datensammlung, wenn sie strukturiert ist ... (manuelle Datei).]“.

Der Entwurf verfehlt das Ziel, die Richtlinie hinsichtlich der Regelung manuell verarbeiteter Daten umzusetzen vor allem deshalb, weil er keine entsprechende Kompetenzbestimmung für den Bundesgesetzgeber vorsieht. Dementsprechend werden die wenigen Stellen im Entwurf, wo manuelle Dateien erwähnt sind, in eckige Klammern gesetzt. Die Begründung, man habe „deshalb keine Aussage über die verfassungsrechtliche Kompetenz ... getroffen, weil es wünschenswert wäre, die diesbezüglichen Bestimmungen den Art. 10 - 15 B-VG einzugliedern“ überzeugt wenig. Es hätte nichts dagegen gesprochen, daß das Bundeskanzleramt mit dem Entwurf einen entsprechenden Textvorschlag für eine Novelle dieser Artikel vorgelegt hätte.

Die ARGE DATEN fordert daher mit Nachdruck, daß das neue DSG in allen seinen Teilen unzweifelhaft auch strukturierte manuelle Datenverarbeitungen umfaßt. Insbesondere im zentralen Punkt der Definition von „Verarbeitung“ und „Datei“ soll man daher möglichst buchstabengetreu der Richtlinie folgen.

3. Begriffsklarheit

An § 3 des Entwurfs kann man am deutlichsten sehen, daß der Versuch, das veraltete Begriffskonzept des DSG beizubehalten und dennoch das Gesetz an die Richtlinie anzupassen, zum Scheitern verurteilt ist.

In den 70er-Jahren konnte man zwischen Erheben, Erfassen, Speichern, Verarbeiten, Benützen, Ausgeben, Übermitteln und Überlassen von Daten noch unterscheiden. Moderne Datenverarbeitungen arbeiten nicht nach diesen linearen Konzepten, sondern stellen Vernetzung und objektorientiertes Programmieren in den Vordergrund. Dementsprechend definiert die Richtlinie einen umfassenden Begriff von „Verarbeitung“ (Art. 2 lit. b) und macht ihn zum zentralen Begriff. Dieser Begriff umfaßt alle maßgeblichen Vorgänge, insbesondere das Erheben, das Speichern, die Benutzung und auch die Übermittlung oder das Vernichten von Daten.

Das neue DSG sollte diese umfassende Begriffsdefinition „Verarbeitung personenbezogener Daten (Verarbeitung)“ möglichst wörtlich aus der Richtlinie übernehmen und im übrigen Gesetzestext nach Möglichkeit immer auf diesen Begriff der „Verarbeitung“ abstellen.

Ganz allgemein wäre es empfehlenswert und auch europarechtlich im Sinne der vom EuGH verlangten notwendigen Rechtsklarheit beim Rechtsanwender geboten, die Definitionen möglichst wörtlich aus der Richtlinie zu übernehmen (siehe Brühann/Zerdick, Umsetzung der EG-Datenschutzrichtlinie in Österreich, Computer & Recht 1996, 556 (557)).

Die Verfasser des Entwurfs versuchen demgegenüber beharrlich, die Begriffszersplitterung in § 3 aufrechtzuerhalten und geraten dabei zu kuriosen Ergebnissen. Zentraler Begriff des Entwurfs ist neuerdings das „Verwenden von Daten“, worin das Ermitteln, Verarbeiten, Übermitteln oder Überlassen von Daten sowie das Mitteilen von Daten an den Betroffenen umfaßt ist (§ 3 Z 14). Daß dieser neue Zentralbegriff erst als vierzehnter von siebzehn Begriffen definiert wird, darf den Leser nicht weiter stören. Der frühere Zentralbegriff des DSG – „Datenverarbeitung“ – wird nun als „Summe von Daten**verwendungs**schritten“ definiert (§ 3 Z 7). **Damit gelangt man zum seltsam anmutenden Ergebnis, daß vom Begriff „Verarbeiten von Daten“ (§ 3 Z 9) das Ermitteln und Übermitteln nicht umfaßt ist, vom Begriff „Datenverarbeitung“ (§ 3 Z 7) aber schon.** Welcher der beiden Begriffe ist wohl gemeint, wenn in § 1 Abs. 4 oder in § 3 Z 4 und 5 von „Verarbeitung“ gesprochen wird?

Eine gegenüber der letzten Fassung des Entwurfs neue Unklarheit ist den Autoren bei der Überarbeitung des Begriffs „Verarbeiten von Daten“ (§ 3 Z 9) passiert: Obwohl dieser Begriff nach dem Willen der Autoren (S. 11 der Erläuterungen) das Ermitteln nicht umfassen soll, umfaßt er nun doch „jede andere Art der Handhabung von Daten ..., soweit es sich nicht um das Überlassen (Z 11) oder Übermitteln (Z 12) oder um die Weitergabe von Daten an den Betroffenen handelt“. Also ist das Ermitteln doch ein Teil des Verarbeitens?

4. Zweistufige Zulässigkeitsprüfung

Die Richtlinie gliedert die Prüfung der Zulässigkeit von Verarbeitungen in zwei Stufen („Doppelprüfung“, Brühann/Zerdick aaO, 558):

Zunächst wird in Art. 6 verlangt, daß Daten bestimmte Qualitätskriterien erfüllen. Insbesondere müssen Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Daten müssen sachlich richtig sein und, wenn nötig, auf den neuesten Stand gebracht werden. Sie dürfen nicht länger als notwendig aufbewahrt werden.

Erst in einem zweiten Schritt wird die Zulässigkeit der Verarbeitung geprüft, wobei Sonderregelungen für sensible Daten und journalistischen Daten getroffen werden.

Der Entwurf setzt dieses Konzept nur mangelhaft um. Bei der ersten Stufe bleibt er hinter den Anforderungen der Richtlinie zurück. **Die Richtlinie wird nicht ausreichend umgesetzt, wenn die Anforderungen an die Qualität der Daten als bloße Soll-Bestimmung formuliert sind.** Bei der zweiten Stufe übernimmt der Entwurf die Doppelprüfung zwar in gewisser Weise in § 6 (Ermittlung und Verarbeitung), wo in den ersten beiden Absätze auf die „Einhaltung der Grundsätze des § 5“ verwiesen wird, nicht aber in § 6 Abs. 5 (Ermittlung und Verarbeitung für ausschließlich private Zwecke). Unklar ist bei der Formulierung des Entwurfs auch, ob die Qualitätskriterien für jene Verarbeitungen gelten, die nicht in den §§ 6 und 7, sondern im 7. Abschnitt (Besondere Vorschriften für einzelne Kategorien von Datenverarbeitungen) geregelt sind.

Die ARGE DATEN fordert daher, den Entwurf in diesem Bereich massiv zu überarbeiten. Dabei sollen die folgenden Grundsätze beachtet werden:

a) Wie in der Richtlinie sollen die „Grundsätze in bezug auf die Qualität der Daten“ an den Beginn gestellt werden, wobei unzweifelhaft klar gestellt sein muß, daß diese Grundsätze jeweils für *alle Formen von Verarbeitungen* gelten und daß es sich um *verbindliche* Anforderungen an die Datenqualität handelt (in unserem Textvorschlag unten: § 5).

b) Danach sollen die verschiedenen Erlaubnistatbestände abgeprüft werden, wobei es zweckmäßig erscheint, diese nicht nach Ermittlung/Verarbeitung/Übermittlung zu gliedern, sondern nach der Art der Verarbeitung (grundsätzliche Regelung/private Datenverarbeitung/sensible Daten/...).

c) Dabei muß darauf geachtet werden, daß Verarbeitungen, die der Verwaltung im Sinne des Art. 18 Abs. 1 B-VG (oder der Gerichtsbarkeit) zuzurechnen sind, „nur auf Grund der Gesetze“ vorgenommen werden dürfen. Diese verfassungsrechtliche Vorgabe soll das DSG wie bisher aufgreifen.

5. Institutionenreform

Die ARGE DATEN regt an, im Zuge der Neuregelung des DSG die Datenschutz-Institutionen grundlegend zu reformieren. Derzeit stellen sich vor allem folgende Problembereiche dar:

a) Im öffentlichen Bereich sind die datenschutzrechtlichen Zuständigkeiten bei der Datenschutzkommission und dem im Bundeskanzleramt angesiedelten Datenschutzbüro konzentriert. Die Leiterin des Datenschutzbüros (welches auch für die Öffentlichkeitsarbeit etc. zuständig ist) ist in Personalunion auch Mitglied der Datenschutzkommission (welche objektiv und unvoreingenommen entscheiden soll). Die Datenschutzkommission selbst hat nicht nur Entscheidungskompetenzen, sondern muß gemäß § 29 Abs. 3 auch als Gutachter bzw. gemäß § 29 Abs. 4 auch als Nebenintervenient auf Seiten des Betroffenen (also als Partei) in Gerichtsverfahren auftreten. Das heißt, daß die selbe Behörde einmal eine Funktion ausübt, in der sie wie der Verwaltungsgerichtshof sogar obersten Organen übergeordnet ist, und dann wieder eine Funktion, in der sie einem Richter des Landesgerichts untergeordnet ist.

   Diese personelle Verschränkung und die Vermischung von Entscheidungs- und Ombudsmannkompetenzen in einer Behörde führt dazu, daß die Datenschutzkommission im Bereich ihrer advokativen Funktionen ziemlich zurückhaltend

agiert: Die Anzahl der von der Datenschutzkommission durchgeführten Systemprüfungen gemäß § 41 DSG ist sehr gering. Dort, wo Prüfungen durchgeführt werden, befaßt die DSK tunlichst nicht die Öffentlichkeit mit den Ergebnissen. Der ARGE DATEN ist kein Fall bekannt, in dem die DSK gemäß § 15 DSG von Amts wegen ein Prüfungsverfahren eingeleitet hätte.

b) Im privaten Bereich ist die Anzahl der Gerichtsverfahren praktisch gleich Null. Nur in etwa 26 Entscheidungen des OGH spielen Datenschutzfragen eine – wenn auch untergeordnete – Rolle. Daran konnte auch die Möglichkeit der Unterstützung durch die DSK (als Nebenintervenientin) nichts ändern.

Die ARGE DATEN schlägt zur Verbesserung der Wirksamkeit der datenschutzrechtlichen Institutionen folgende Reformen vor:

a) Die Trennung der Zuständigkeiten zwischen DSK und Gerichten soll an sich beibehalten werden. Streitigkeiten zwischen betroffener Person und Verantwortlichem der Verarbeitung sind im wesentlichen zivilrechtliche Auseinandersetzungen, für die das Instrumentarium der Zivilgerichtsbarkeit besser geeignet ist als ein Verfahren nach dem AVG. Dies gilt auch für die Durchsetzung der Auskunftserteilung. Es ist nicht einsichtig, warum gerade das Auskunftsrecht (und nicht etwa das Richtigstellungsrecht oder die Durchsetzung der Informationspflicht) in die alleinige Zuständigkeit der DSK übergehen sollen. Da in der Praxis oft Auskunfts- und Richtigstellungs- bzw. Löschungsansprüche nebeneinander geltend gemacht werden (z. B. bei unvollständigen Auskünften), sollte das Verfahren nicht auseinandergerissen werden.

b) Im Bundeskanzleramt soll ein unabhängiger Bundesdatenschutzbeauftragter eingerichtet werden, welcher aktiv advokative Kompetenzen wahrnimmt, Anlaufstelle für Datenschutzfragen aller Art ist, Öffentlichkeitsarbeit betreibt und die in Art. 28 Abs. 3 der Richtlinie beschriebenen Kontrollbefugnisse wahrnimmt. Der Bundesdatenschutzbeauftragte soll bei festgestellten Verstößen gegen das DSG Beschwerde bei der DSK oder Klage bei Gericht erheben.

Die Kompetenzen der DSK hingegen sollen auf die Rolle einer Entscheidungsinstanz mit Tribunalcharakter im Beschwerde-, Registrierungs- und Genehmigungsverfahren beschränkt werden.

Damit würde an die Stelle des derzeitigen (und im Entwurf verstärkten) inquisitorischen Prinzips, bei dem die DSK Kontrollbefugnisse ausübt und dann bei sich selbst ein Verfahren einleitet (§ 26 Abs. 3 des Entwurfs), ein kontradiktorisches DSK-Verfahren zwischen dem Bundesdatenschutzbeauftragten und der belangten Behörde treten.

Die vorgeschlagene Trennung in advokative und Entscheidungskompetenzen würde dem Datenschutz insgesamt nützen, da ein Datenschutzbeauftragter, der über die von ihm eingeleiteten Verfahren nicht selbst entscheiden muß, viel aktiver auftreten kann und nicht noble Zurückhaltung üben muß.

c) Im privaten Bereich soll für die betroffenen Personen die Schwelle der Rechtsdurchsetzung abgesenkt werden. Vorbild sollen dabei die Regelungen des Mietrechts, Arbeitsrechts und des Konsumentenschutzes sein. Im Detail:

   – Statt den Landesgerichten sollen die Bezirksgerichte zuständig gemacht werden.

   – Als Streitwert soll (außer bei Klagen auf Schadenersatz) ein niedriger fiktiver Streitwert fixiert werden, sodaß für den Kläger kein Anwaltszwang besteht.

   – Wie im Mietrecht sollte der vertretende Beistand einer Datenschutzorganisation möglich sein.

Ein ungelöstes Problem ist nach wie vor die Ahndung von Datenschutzverletzungen durch ein Gericht. In der Praxis wurde der ARGE DATEN z. B. der Fall eines von einem Gericht im Rahmen einer Fahrnisexekution gepfändeten und versteigerten Computers bekannt, bei dem der Verdacht bestand, daß das Gericht die auf der Festplatte des Computers befindlichen personenbezogenen Daten nicht gelöscht hat. **Derzeit ist für die Überprüfung solcher Fälle niemand zuständig, was dem rechtsstaatlichen Prinzip kraß widerspricht.** Die ARGE DATEN schlägt die Möglichkeit einer Beschwerde an das organisatorisch übergeordnete Gericht vor.

6. Materielles Datenschutzrecht

Eine Reihe der von der Richtlinie vorgesehenen Neuerungen des materiellen Datenschutzrechts werden vom Entwurf nicht oder nur nachlässig umgesetzt. Dies betrifft:

- § 21 Informationspflicht: Der Entwurf nimmt einen großen Teil der Datenverarbeitungen aus und sieht einen Teil der Informationsverpflichtung (z. B. Belehrung über Auskunfts- und Berichtigungsrechte und darüber, ob die Beantwortung der Fragen durch den Betroffenen verpflichtend ist) nicht vor.

- § 23 Auskunftsrecht: Es fehlt das Recht auf Auskunft über den logischen Aufbau automatisierter Verarbeitungen.

- § 25 Widerspruchsrecht: Das Widerspruchsrecht gegen Datenverarbeitungen für Zwecke der Direktwerbung wird nicht umgesetzt.

Die ARGE DATEN fordert eine kompromißlose Umsetzung aller Neuerungen und Verbesserungen, die die Richtlinie im Bereich des materiellen Datenschutzrechts vorsieht.

7. Trennung öffentlicher / privater Bereich

Die ARGE DATEN begrüßt, daß dem Vorbild der Richtlinie entsprechend die Trennung zwischen öffentlichem und privatem Bereich grundsätzlich aufgehoben wurde. Die in diesem Zusammenhang in der Vergangenheit aufgetretenen Probleme wurden jedoch nicht restlos beseitigt.

Insbesondere erwies sich die Formulierung des § 1 Abs. 6 – „Soweit Rechtsträger in Formen des Privatrechts tätig sind, ist das Grundrecht auf Datenschutz *im ordentlichen Rechtsweg geltend zu machen*.“ als problematisch, da diese Verfassungsbestimmung auch innerhalb einer Behörde eine schwer auszumachende Trennlinie zwischen hoheitlichen und privatwirtschaftlichen Datenverarbeitungen zieht. Dieses Problem besteht auch bei der vorgeschlagenen Neuformulierung des § 1 Abs. 6 bei jenen Behörden weiter, die z. B. als GmbH eingerichtet sind (Telekom-Control-GmbH, AMS, ...). Soweit diese in Vollziehung der Gesetze tätig werden, sind sie dem öffentlichen Bereich zuzurechnen und die DSK ist für sie zuständig, soweit sie privatwirtschaftlich z. B. Büroorganisationsprogramme verwenden, gehören sie zum privaten Bereich und nach der Textierung des neuen § 1 Abs. 6 ist „das Grundrecht auf Datenschutz *im Zivilrechtsweg geltend zu machen*“.

Dieses Problem entsteht dadurch, daß auf verfassungsrechtlicher Ebene eine Behördenzuständigkeit (Verwaltungsbehörde/Zivilrechtsweg) festgelegt wird. Der Sinn des § 1 Abs. 6 liegt aber darin, das Grundrecht mit einer Drittwirkung auszustatten.

Zur Lösung dieses Problems wird vorgeschlagen, drei Fragestellungen zu unterscheiden:

a) **Drittwirkung**: § 1 Abs. 6 soll bloß bezwecken, daß das Grundrecht auf Datenschutz (anders als andere Grundrechte) nicht nur gegenüber dem Staat, sondern auch gegenüber Rechtsträgern des Privatrechts gilt. Dafür ist es aber nicht erforderlich, den „Zivilrechtsweg“ anzusprechen und damit die oben genannten verfassungsrechtlichen Probleme aufzuwerfen. Es genügt, eine Formulierung zu wählen, die ausschließlich die Drittwirkung zum Inhalt hat; etwa „Das Grundrecht auf Datenschutz gilt auch gegenüber Rechtsträgern, die in Formen des Privatrechts tätig sind.“

b) **Behördenzuständigkeit**: Die Regelung der Zuständigkeit für die Durchsetzung des Grundrechtes sollte dem einfachen Gesetzgeber vorbehalten bleiben und möglichst so erfolgen, daß in der Praxis jeweils für einen Auftraggeber ausschließlich eine Behörde zuständig ist, d. h. für einen in Vollziehung der Gesetze tätigen Rechtsträger jedenfalls die Datenschutzkommission (auch wenn es sich im konkreten Einzelfall um eine Verarbeitung in Formen des Privatrechts handelt) und für einen überhaupt nie in Vollziehung der Gesetze tätigen Rechtsträger jedenfalls ein Gericht. Das ist auch die derzeit geltende (allerdings dem § 1 Abs. 6 DSG widersprechende) Zuständigkeit.

c) **Zulässigkeitsvoraussetzungen**: Aufgrund des verfassungsrechtlichen Legalitätsprinzips (Art. 18 Abs. 1 B-VG: „Die gesamte staatliche Verwaltung darf nur auf Grund der Gesetze ausgeübt werden.“) dürfen hoheitliche Datenverarbeitungen (mögen sie nun von einem Rechtsträger des öffentlichen Rechts oder des Privatrechts ausgeübt werden) jedenfalls nur auf gesetzlicher Grundlage erfolgen. Hingegen können bei Datenverarbeitungen, die nicht im hoheitlichen Bereich erfolgen (etwa in der Büroverwaltung einer Behörde, bei der Vergabe öffentlicher Aufträge und Subventionen oder beim Versand von Informationsmaterial) auch andere Zulässigkeitsvoraussetzungen wie der „berechtigte Zweck“ oder die „Zustimmung des Betroffenen“ als Zulässigkeitsvoraussetzung einer Datenverarbeitung herangezogen werden.

Bei der legistischen Umsetzung dieser Grundsätze ist es empfehlenswert, die Formulierung „öffentlicher Bereich“ zu vermeiden, da sich die hier unter b) und c) vorgeschlagenen Abgrenzungen unterscheiden. Unter b) lautet die Frage, welchem Bereich der *Auftraggeber* zuzurechnen ist, unter c)

hingegen, welchem Bereich die *Verarbeitung* zuzurechnen ist. Textvorschläge sind im besonderen Teil wiedergegeben.

8. Kompetenzrecht

Es stellt einen schweren Mangel des Entwurfs dar, daß er die Klärung der kompetenzrechtlichen Grundlage für ein neues Datenschutzgesetz offenläßt. Ein wesentlicher Punkt der Richtlinie, nämlich die Einbeziehung der manuellen Dateien in die Datenschutzgesetzgebung, kann nur dann sinnvoll umgesetzt werden, wenn es eine einheitliche bundesgesetzliche Regelung gibt. Eine Aufsplitterung des Datenschutzes in zehn verschiedene Gesetze (1 Bundesgesetz für automationsunterstützt verarbeitete Daten, 9 Landesgesetze für manuell verarbeitete Daten) würde die ohnehin komplexe Materie völlig unüberschaubar machen.

Für die kompetenzrechtliche Grundlage schlagen wir vor, an die Stelle des bisher in § 2 DSG verwendeten Begriffs „Angelegenheiten des Schutzes personenbezogener Daten im *automationsunterstützten* Datenverkehr“ einfach den Begriff „Angelegenheiten des Datenschutzes“ bzw. „Datenschutz“ zu setzen. Die Gesetzgebung soll in diesem Bereich dem Bund zufallen (wodurch die Bundeskompetenz um den Datenschutz betreffend nicht automationsunterstützter Daten erweitert wird), die Vollziehung entsprechend dem bisherigen § 2 Abs. 2 DSG aufgeteilt werden.

Dies bedeutet eine geringfügige Kompetenzerweiterung für den Bund, soweit manuell verarbeitete Daten umfaßt sind. Geringfügig ist diese Erweiterung deshalb, weil weite Bereiche der Datenschutzgesetzgebung ohnehin auf andere Bundeskompetenzen gestützt werden können: Soweit Daten von Rechtsträgern des Privatrechts verarbeitet werden, tauchen zwischen Datenverarbeiter und Betroffenem typisch zivilrechtliche Probleme auf, die (wie z. B. § 16 ABGB oder der Bildnisschutz im Urheberrecht) unter die Zivilrechtskompetenz des Bundes fallen. Die von Landesbehörden verarbeiteten Daten können großteils durch die bestehende Bedarfskompetenz des Bundes im Bereich des Verwaltungsverfahrens einheitlich geregelt werden. Die Datenschutzkommission hat ihre eigene verfassungsrechtliche Grundlage. Die Gerichte fallen selbstverständlich unter die Bundeskompetenz. Den Ländern verbleibt daher nach der *bestehenden* Kompetenzrechtslage nur die datenschutzrechtliche Regelung mancher manuellen Datenverarbeitungen von Landesbehörden sowie allenfalls die Regelung der Registrierungspflicht von manuellen Datenverarbeitungen.

Aus verfassungsrechtlichen Überlegungen wäre es wünschenswert, wenn alle kompetenzrechtlichen Bestimmungen in den Art. 10 bis 15 B-VG versammelt wären.

Eigentlich hätte schon 1978 verfassungsrechtlich vorgesehen werden sollen, daß Angelegenheiten des Datenschutzes unmittelbar von Bundesbehörden (DSK, DVR, Bundeskanzler) versehen werden dürfen, ohne daß in erster Instanz der Landeshauptmann in mittelbarer Bundesverwaltung zuständig ist (Art. 102 B-VG). Das sollte jetzt saniert werden.

B. Besonderer Teil (mit Textvorschlägen)

§ 1 – Grundrecht auf Datenschutz

Zunächst sei auf die im allgemeinen Teil (A. 1.) ausgeführten Vorschläge verwiesen, das Grundrecht stärker in Richtung eines Rechtes auf informationelle Selbstbestimmung zu akzentuieren und es auf natürliche Personen zu beschränken. – Zur Drittwirkung (§ 1 Abs. 6) siehe das oben (A. 7.) zur Trennung öffentlicher/privater Bereich Gesagte.

Die ARGE DATEN begrüßt, daß das Grundrecht um einige Punkte aus der Richtlinie erweitert werden soll, sodaß auch die Regelung der sensiblen Daten (Art. 8) und das Widerspruchsrecht (Art. 14 lit. a) der Richtlinie) grundrechtlich verankert werden.

Diesem Gedanken entsprechend sollten auch die übrigen Neuerungen der Richtlinie in das Grundrecht aufgenommen werden: Das betrifft insbesondere den dem Informationsrecht der Art. 10 und 11 zugrundeliegenden Gedanken, daß die betroffene Person darüber informiert werden sollte, welche Daten über sie verarbeitet werden. Weiters sollte auch das Recht auf Auskunft über den logischen Aufbau der automatisierten Verarbeitung (Art. 12 lit. a) dritter Gedankenstrich) grundrechtlich verankert werden.

Zur Legistik: Da in § 1 Begriffe verwendet werden, deren Definition in § 3 verändert wurde, muß es in § 3 statt „Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten:“ richtigerweise „Im Sinne dieses Bundesgesetzes bedeuten:“ heißen.

Textvorschlag:

Grundrecht auf Datenschutz

(Verfassungsbestimmung)

§ 1. (1) Jede natürliche Person hat Anspruch auf Selbstbestimmung bei der Verarbeitung sie betreffender personenbezogener Daten, soweit sie daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung ihres Privat- und Familienlebens hat.

(2) Beschränkungen des Rechtes nach Abs. 1 durch Verarbeitung personenbezogener Daten sind nur zur Wahrung berechtigter Interessen eines anderen oder auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (BGBl. Nr. 210/1958) genannten Gründen notwendig sind. Auch im Falle solcher zulässiger Beschränkungen darf nur die jeweils gelindeste zielführende Art des Eingriffs in das Grundrecht gewählt werden.

(3) Die Verarbeitung von Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben ist unzulässig, soweit sich aus gesetzlichen Vorschriften nicht anderes ergibt. Derartige Vorschriften müssen zur Wahrung wichtiger öffentlicher Interessen notwendig sein und angemessene Garantien vorsehen.

(4) Jede natürliche Person hat, soweit sie betreffende Daten automatisiert oder in Dateien verarbeitet werden,
1. das Recht, über die Verarbeitung informiert zu werden;
2. das Recht auf Auskunft darüber, wer sie betreffende personenbezogene Daten verarbeitet, was die Zweckbestimmung dieser Verarbeitung ist, woher die Daten stammen, welcher Art und welchen Inhalts die Daten sind und an wen sie übermittelt werden sowie bei automatisierten Verarbeitungen über den logischen Aufbau der Verarbeitung, und
3. das Recht auf Richtigstellung unrichtiger, unaktueller oder unvollständiger und Löschung unzulässigerweise verarbeiteter Daten. Darüber hinaus sind auch überwiegende, sich aus der besonderen Situation des Betroffenen ergebende Gründe bei der Entscheidung über ein Löschungsbegehren zu berücksichtigen.

Die Ausübung dieser Rechte kann durch besondere Gesetze geregelt werden.

(5) Beschränkungen der Rechte nach Abs. 4 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(6) Das Grundrecht auf Datenschutz gilt auch gegenüber Rechtsträgern, die in Formen des Privatrechts tätig sind.

Der in diesem Vorschlag verwendete Verarbeitungsbegriff entspricht dem umfassenden Begriff der Richtlinie.

§ 2 (alt) – Kompetenzrecht

Im Sinne des oben unter A. 8. Gesagten schlagen wir für die Formulierung der kompetenzrechtlichen Grundlage eine Einbettung in das Bundes-Verfassungsgesetz vor:

Artikel 10. (1) Bundessache ist die Gesetzgebung und die Vollziehung in folgenden Angelegenheiten: ...

... Datenschutz, soweit er nicht unter Artikel 11 fällt,

Aufgrund des Naheverhältnisses zu Bestimmungen des Zivilrechts (Datenschutzregelungen des privaten Bereichs) und der

Verwaltungsgerichtsbarkeit (Datenschutzkommission) wäre eine Einbettung in Z. 6, z. B. zwischen den bestehenden Kompetenztatbeständen „Verwaltungsgerichtsbarkeit“ und „Urheberrecht“ sinnvoll.

Artikel 11. (1) Bundessache ist die Gesetzgebung, Landessache die Vollziehung in folgenden Angelegenheiten:

8. Datenschutz, soweit personenbezogene Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verarbeitet werden, und soweit nicht durch Bundesgesetz der Bundesdatenschutzbeauftragte, die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Artikel 102. (2) Folgende Angelegenheiten können im Rahmen des verfassungsmäßig festgestellten Wirkungsbereiches unmittelbar von Bundesbehörden versehen werden:

..., Datenschutz, ...

Alternativvorschlag: Kompetenzbestimmung wie bisher im DSG:

[Artikel 1. (Verfassungsbestimmung) ...]

Zuständigkeit zur Gesetzgebung und Vollziehung

§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Datenschutzes.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit personenbezogene Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verarbeitet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz der Bundesdatenschutzbeauftragte, die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden. Angelegenheiten des Datenschutzes können unmittelbar von Bundesbehörden versehen werden.

§ 2 (neu) – Anwendungsbereich

Der ARGE DATEN ist völlig unverständlich, wieso eine bloß den Anwendungsbereich regelnde Bestimmung im Verfassungsrang beschlossen werden soll. Dafür besteht überhaupt kein Bedarf. Richtigerweise sollte bloß das Grundrecht (§ 1) im Verfassungsrang stehen.

Eine Gliederung des DSG in zwei Artikel (Artikel 1: §§ 1 und 2 im Verfassungsrang, Artikel 2: Rest) erübrigt sich.

§ 3 – Definitionen

Wie bereits oben unter A. 3. ausgeführt, sollten schon aus Gründen der notwendigen Rechtsklarheit die Definitionen möglichst wörtlich aus der Richtlinie übernommen werden.

Am vorgeschlagenen Entwurf ist neben dem oben kritisierten Begriffswirrwarr unter anderem folgendes zu beanstanden:

Z 1 Daten: Die Formulierung „ohne unverhältnismäßigen Aufwand“ entspricht nicht der Definition der Richtlinie.

Z 4 Auftraggeber und Z 5 Dienstleister: Beide Definitionen verwenden den Begriff „automationsunterstützte Verarbeitung“, bei welchem unklar ist, ob damit die „automationsunterstützte Datenverarbeitung“ oder das „Verarbeiten von Daten“ gemeint ist.

Z 7 Datenverarbeitung: Kein Leser dieser Definition wird auf Anhieb verstehen, daß mit der Datenverarbeitung etwas ganz anderes gemeint ist als mit dem Verarbeiten von Daten (Z. 9). Unverständlich ist auch, weshalb die Definition im ersten Halbsatz umständlich das Kriterium der automationsunterstützten Verarbeitung hervorhebt („zur Gänze oder auch nur teilweise“ ... „also maschinell und programmgesteuert“), obwohl sich im zweiten Halbsatz dann zeigt, daß es darauf ohnehin nicht ankommt. Die Formulierung der Richtlinie: „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang ... im Zusammenhang mit personenbezogenen Daten“ sagt viel klarer, worum es eigentlich geht.

Z 9 Verarbeiten von Daten: Der neu eingefügte Halbsatz „jede andere Art der Handhabung von Daten einer Datenverarbeitung ..., soweit es sich nicht um das Überlassen (Z 11) oder Übermitteln (Z 12) oder um die Weitergabe von Daten an den Betroffenen handelt“ umfaßt – wohl gegen den Willen der Autoren des Entwurfs – auch das Ermitteln von Daten, weshalb die in der Folge permanent verwendeten Begriffspaare „ermitteln und/oder verarbeiten“ redundant werden.

Z 12 Übermitteln von Daten: Die Phrase „Weitergabe von Daten *im Rahmen oder aus* einer Datenverarbeitung“ zeigt deutlich, daß den Verfassern des Entwurfs noch nicht ganz klar war, ob das Übermitteln begrifflich zur „Datenverarbeitung“ dazugehört („im Rahmen“) oder nicht („aus“).

Für den Leser unverständlich ist vor allem die Reihung der Begriffe, die sich am alten DSG orientiert und darunter leidet, daß der vierzehnte Begriff (Verwenden von Daten) zum

Verständnis der meisten davor definierten Begriffe notwendig ist.

Der folgende alternative Textvorschlag orientiert sich so weit wie möglich wörtlich an der Richtlinie. Da die Definitionen auch für das Grundrecht und den Anwendungsbereich gelten sollen, darf es im Einleitungssatz nicht „Im Sinne der *folgenden Bestimmungen* dieses Bundesgesetzes bedeuten:“ heißen.

Definitionen

§ 3. Im Sinne dieses Bundesgesetzes bedeuten:

1. personenbezogene Daten: alle Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

2. sensible Daten: personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben;

3. Verarbeitung personenbezogener Daten (Verarbeitung): jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;

4. Datei mit personenbezogenen Daten (Datei): jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird;

5. für die Verarbeitung Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

6. Auftragsverarbeiter; die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

7. Dritter: die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

8. Empfänger: die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die Daten erhält, gleichgültig, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines

einzelnen Untersuchungsauftrags möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger;

9. Einwilligung der betroffenen Person: 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;

10. Übermitteln von Daten: die Weitergabe von Daten aus einer Verarbeitung an einen Dritten (Z 7), insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;

11. Überlassen von Daten: die Weitergabe von Daten vom für die Verarbeitung Verantwortlichen an einen Auftragsverarbeiter oder zwischen Auftragsverarbeitern.

12. Inland: das österreichische Staatsgebiet sowie jene Orte außerhalb Österreichs, an welchen gemäß Völkerrecht die österreichische Rechtsordnung anzuwenden ist;

13. Niederlassung: eine durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die tatsächlich Tätigkeiten ausübt.

Dieser Textvorschlag übernimmt auch die Begriffe „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, obwohl man hier durchaus auch die Begriffe „Auftraggeber“ und „Dienstleister“ beibehalten könnte.

Der bislang in § 3 Z 4 und 5 verwendete Begriff „Organ einer Gebietskörperschaft“ erscheint bei näherer Betrachtung der üblichen Auslegung dieses Begriffs falsch. Normalerweise wird nämlich ein Organ, das „für den Bundesminister“ zeichnungsberechtigt ist, nicht als eigenständiger Auftraggeber neben dem Bundesminister angesehen. Eine Abgrenzung verschiedener Auftraggeber des öffentlichen Rechts wird vielmehr dort vorgenommen, wo die Auftraggeber unterschiedliche Kompetenzen haben. Dies entspricht aber nicht dem Organbegriff, sondern dem Behördenbegriff. Daher erscheint die von der Richtlinie gewählte Formulierung „Behörde“ auch als richtiger.

Zu Z 13 (Niederlassung) sollte in den Erläuterungen unbedingt das Problem erörtert werden, daß ein Computer in Österreich aufgestellt und aus dem Ausland mittels Fernwartung betrieben werden kann. Ein solcher Rechner benötigt bei entsprechender Konfiguration überhaupt kein in Österreich anwesendes Personal des Betreibers (evtl. mit Ausnahme einer Person, die ihn im Fall eines Systemabsturzes aus- und wieder einschaltet). Es ist jedenfalls zu klären, ob es sich bei einem solchen Gerät um eine „Niederlassung“ im Sinne des DSG handelt.

§ 4 – Öffentlicher und privater Bereich

Wie oben unter A. 7. ausgeführt wurde, sollten Definitionen von „öffentlicher Bereich“ und „privater Bereich“ besser

vermieden werden, da sie nur verfassungsrechtliche Probleme aufwerfen.

§ 4 Abs. 2 Z 2 des Entwurfs sieht offenbar vor, daß ein Auftraggeber auch teilweise in den öffentlichen und teilweise in den privaten Bereich fallen kann (arg. „soweit“ – diese Auslegung wäre im Hinblick auf § 1 Abs. 6 auch verfassungsrechtlich geboten). In § 4 Abs. 1 hingegen geht der Entwurf davon aus, daß klar ist, ob ein Auftraggeber dem öffentlichen Bereich zuzurechnen ist oder nicht.

Es wird daher vorgeschlagen, § 4 ersatzlos zu streichen und die relevanten Bestimmungen folgendermaßen zu formulieren:

a) Drittwirkung

§ 1 Abs. 6: Das Grundrecht auf Datenschutz gilt auch gegenüber Rechtsträgern, die in Formen des Privatrechts tätig sind.

Eine Abgrenzung der Bereiche ist hier nicht nötig. Es geht bloß um die Drittwirkung des Grundrechts.

b) Behördenzuständigkeit

§ 26a. (1) Ansprüche wegen Verletzung der Rechte nach diesem Bundesgesetz oder nach datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates der Europäischen Union, die gemäß § 2 im Inland Anwendung finden, sind

1. mit Beschwerde an die Datenschutzkommission (§ 27) geltend zu machen, wenn sie sich gegen einen Rechtsträger des öffentlichen Rechts oder einen in Vollziehung der Gesetze tätigen Rechtsträger des Privatrechts richten und das verletzende Verhalten nicht ein Akt der Gerichtsbarkeit oder der Gesetzgebung ist;
2. auf dem ordentlichen Rechtsweg (§ 28) geltend zu machen, wenn sie sich gegen einen nicht in Vollziehung der Gesetze tätigen Rechtsträger des Privatrechts richten;
3. mit Beschwerde an das organisatorisch übergeordnete Gericht (§ 28a) geltend zu machen, wenn das verletzende Verhalten ein Akt der Gerichtsbarkeit ist.

(2) Schadenersatzansprüche sind jedenfalls auf dem ordentlichen Rechtsweg geltend zu machen.

§ 30 (1) (Verfassungsbestimmung) Die Datenschutzkommission entscheidet:

1. über Beschwerden von Personen, die behaupten, in ihren Datenschutzrechten verletzt worden zu sein, soweit das verletzende Verhalten einem Rechtsträger des öffentlichen Rechts oder einem in Vollziehung der Gesetze tätigen Rechtsträger des privaten Rechts zuzurechnen ist und soweit dieses Verhalten nicht ein Akt der Gerichtsbarkeit oder der Gesetzgebung ist;

Diese Abgrenzung soll jeweils klar die Behördenzuständigkeit regeln. Es sollen für jeden Rechtsträger jeweils eindeutig entweder die Datenschutzkommission oder die Gerichte zuständig sein. Hingegen soll es keine Rolle spielen, ob die Datenverarbeitung eine hoheitliche Datenverarbeitung ist. Die Formulierung lehnt sich bewußt an die bewährte Abgrenzung bei der Amtshaftung an. Wie dort soll ein Rechtsträger im Zweifel dem öffentlichen Bereich

zugerechnet werden, mag er auch nur geringe hoheitliche Befugnisse haben.

c) Zulässigkeitsvoraussetzungen

§ 6 (2) In Vollziehung der Gesetze dürfen Daten unter Einhaltung der Grundsätze des § 5 nur verarbeitet werden, wenn dafür eine ausdrückliche gesetzliche Ermächtigung besteht, oder soweit dies für den für die Verarbeitung Verantwortlichen zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bildet.

Hier wird darauf abgestellt, ob die jeweilige Datenverarbeitung in Vollziehung der Gesetze erfolgt.

§ 5 – Zulässigkeit der Verwendung von Daten

Es ist absolut inakzeptabel, daß der Entwurf die Grundsätze über die Qualität der Daten als bloße Soll-Bestimmung vorsieht. Die Qualitätskriterien stellen einen zentralen Punkt der Richtlinie dar. Entsprechend dem zweistufigen Konzept der Zulässigkeitsprüfung *müssen* zuerst die Qualitätskriterien erfüllt sein (Art. 6), bevor die übrigen Zulässigkeitsvoraussetzungen für eine Verarbeitung geprüft werden (Art. 7 und 8)

Da das neue DSG die Richtlinie umsetzen, also für das österreichische Recht näher ausgestalten sollte, ist es problematisch, wenn das DSG den Richtlinientext verkürzt. Vielmehr sollten sich die Umsetzung der Prinzipien „aufgrund der klaren europarechtlichen Vorgaben eng am gewählten Wortlaut der Richtlinienkataloge orientieren und die gewählten allgemeinen Rechtsbegriffe im Hinblick auf spezifische Verarbeitungssituationen präzisieren“ (Brühann/Zerdick aaO, 558).

Problematisch ist auch die Ersetzung des von der Richtlinie verwendeten Begriffs „nach Treu und Glauben“ durch den Begriff „Übung des redlichen Verkehrs“. Gerade das Wort „Übung“ suggeriert allzu leicht, daß eine Verarbeitung dadurch zulässig wird, daß sie in einem bestimmten Bereich „üblich“ ist.

Die im Entwurf in Abs. 4 vorgeschlagene Pflicht zur Benennung eines in Österreich ansässigen Vertreters ist begrüßenswert, aber noch unausgegoren. Offen bleibt bei diesem Vorschlag, wem gegenüber der Vertreter zu benennen ist (der Datenschutzkommission im Rahmen der Registrierung?) und was die Rechtsfolge sein soll, wenn die Benennung unterbleibt. Gerade für den Fall der unterlassenen Benennung ist eine derartige Bestimmung aber gedacht. Vielleicht wäre eine Übersiedlung dieser Bestimmung in das

Registrierungsverfahren und eine sprachliche Angleichung an § 10 ZustellG sinnvoll.

Der vorgesehene Abs. 5 sollte ersatzlos entfallen. Entsprechend den Prinzipien der österreichischen Bundesverfassung gibt es für die Erzeugung von Rechtsnormen, also verbindlichen Vorschriften, ganz bestimmte Verfahren: die Gesetzgebung im Nationalrat oder Landtag und die Erlassung von Verordnungen durch eine Verwaltungsbehörde. Die Ausarbeitung von „Verhaltensregeln“ durch „Berufsverbände und vergleichbare Einrichtungen“ gehört nicht dazu. Insbesondere ist es nach dem österreichischen Verfassungsrecht nicht zulässig, die nähere Auslegung gesetzlicher Begriffe (hier: „Übung des redlichen Verkehrs“) an eine von der Verfassung nicht dafür vorgesehene und demokratisch nicht legitimierte Institution zu delegieren.

Abgesehen davon ist die Bestimmung auch legistisch mangelhaft, weil das „Bundeskanzleramt“ keine Behörde, sondern bloß der Hilfsapparat für die Behörde „Bundeskanzler“ ist. Daher wird in Gesetzen (zB in den §§ 8, 23, 24, 32 des geltenden DSG) bei behördlichen Kompetenzen prinzipiell vom Bundeskanzler und nie vom Bundeskanzleramt gesprochen. Dem Bundeskanzleramt können nur organisationsrechtliche Kompetenzen zugesprochen werden (zB die Geschäftsführung der DSK gemäß § 35 Abs. 2 DSG).

Textvorschlag:

Grundsätze in Bezug auf die Qualität der Daten

§ 5. (1) Personenbezogene Daten

1. dürfen nur nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

2. müssen für festgelegte eindeutige und rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden.

3. müssen den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen;

4. müssen sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sein; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden;

5. dürfen nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht.

Für die Regelung historischer, statistischer oder wissenschaftlicher Zwecke haben wir vorerst keinen Textvorschlag ausgearbeitet.

(2) Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen. Dies gilt auch dann, wenn er für die Verarbeitung Auftragsverarbeiter heranzieht.

(3) ...

Die im Entwurf vorgesehene Gliederung – 2. Abschnitt: Datenqualität, Ermittlung, Verarbeitung, Übermittlung; 7. Abschnitt: Besondere Kategorien – legt den Gedanken nahe, daß die Qualitätskriterien für die besonderen Kategorien von Datenverarbeitung nicht gelten. Dies wird auch dadurch unterstrichen, daß in den §§ 6 und 7 jeweils mehrmals auf die „Einhaltung der Grundsätze des § 5“ verwiesen wird, im 7. Abschnitt aber nicht. Daher wird eine Gliederung vorgeschlagen, die das der Richtlinie zugrundeliegende Konzept einer zweistufigen Zulässigkeitsprüfung unterstreicht:

2. Abschnitt: Grundsätze in Bezug auf die Qualität der Daten (§ 5 wie oben vorgeschlagen)
3. Abschnitt: Zulässigkeit der Verarbeitung von Daten (§ 6: Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten, wie unten vorgeschlagen; §§ 7ff: Besondere Kategorien der Verarbeitung wie im 7. Abschnitt des Entwurfs)

§ 6 und 7 – Zulässigkeit der Ermittlung / Verarbeitung / Übermittlung von Daten

a) Die vom Entwurf beibehaltene prinzipielle Trennung zwischen Ermittlung und Verarbeitung einerseits und Übermittlung andererseits bewirkt, daß sich einerseits die verschiedenen Erlaubnistatbestände wiederholen (vgl. zB § 6 Abs. 4 mit § 7 Abs. 1), daß aber andererseits nicht nachvollziehbare feine Unterschiede zwischen den Regelungen auftauchen. So ist die Grundstruktur zwischen § 6 und § 7 bei näherer Betrachtung völlig unterschiedlich:

- § 6 verlangt zunächst in Abs. 1 eine gesetzliche Ermächtigung, stellt dieser dann in Abs. 2 den „berechtigten Zweck“ und das Kriterium „überwiegende schutzwürdige Geheimhaltungsinteressen des Betroffenen“ an die Seite und definiert in Abs. 4 dann nähere Bestimmungen zu diesen überwiegenden schutzwürdigen Geheimhaltungsinteressen: Zustimmung des Betroffenen, lebenswichtige Interessen, öffentliche Funktion.

– § 7 ordnet die Kriterien „Zustimmung des Betroffenen“ und „lebenswichtige Interessen“ nicht dem Kriterium „überwiegende schutzwürdige Geheimhaltungsinteressen“ unter, sondern stellt sie daneben.

Daneben fallen auch einige andere Ungereimtheiten ins Auge. So ist z. B. nicht nachvollziehbar, wieso die lebenswichtigen Interessen eines anderen Menschen bei der Ermittlung und Verarbeitung ausdrücklich als Zulässigkeitstatbestand genannt werden (§ 6 Abs. 4 Z 3), nicht aber bei der Übermittlung (§ 7 Abs. 1). Ebenso ist die Ermittlung und Verarbeitung von Daten zulässig, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben (§ 6 Abs. 4 Z 4), die Übermittlung aber offenbar nicht.

b) Der Vorschlag für eine strengere Gesetzesbindung bei „On-line Übermittlungen“ (§ 7 Abs. 2 Z 2 des Entwurfs) ist begrüßenswert, allerdings ist der Begriff „On-line Übermittlung“ unglücklich gewählt. Es ist nämlich datenschutzrechtlich völlig egal, ob eine konkrete Übermittlung z. B. durch Übersendung eines Briefs oder einer Diskette, durch E-Mail, mittels FTP oder Telnet durchgeführt wird.

Datenschutzrechtlich problematisch ist es hingegen, wenn eine gesamte Datenbank (wie z. B. das Zentralmelderegister oder alle Lohn- und Einkommensteuerbescheide der Finanzämter) dem Direktzugriff einer anderen Behörde (wie z. B. der Studienbeihilfenbehörde) geöffnet wird. Damit entsteht für das Personal der abrufenden Stelle die relativ unkontrollierbare Möglichkeit, auf beliebige Datensätze zuzugreifen. Die Hemmschwelle, Datensätze zu lesen, an denen man nicht aus dienstlichen Gründen, sondern bloß aus privater Neugier interessiert ist, sinkt dadurch beträchtlich.

c) Die Regelung der Datenverarbeitung für persönliche und familiäre Tätigkeiten (besser: Zwecke) ist wie bisher in unübersichtlicher Weise über zwei Paragraphen verstreut und sollte in einer Bestimmung zusammengefaßt werden.

d) Im folgenden Textvorschlag wird jeweils vom weiten Verarbeitungsbegriff der Richtlinie ausgegangen. Die Gliederung wurde gegenüber dem Entwurf grundlegend umgestellt.

Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten

§ 6. (1) Daten dürfen unter Einhaltung der Grundsätze des § 5 nur verarbeitet werden, wenn eine der folgenden Voraussetzungen erfüllt ist:

1. die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verarbeitung bewirkt; im Falle der Verarbeitung sensibler Daten muß die Einwilligung ausdrücklich gegeben worden sein;

2. die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;

3. die Verarbeitung ist für die Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

4. die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person oder eines Dritten und die Einwilligung gemäß Z 1 konnte nicht rechtzeitig eingeholt werden;

5. die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß § 1 Abs. 1 geschützt sind, überwiegen. Bei sensiblen Daten ist, sofern sich aus gesetzlichen Vorschriften nicht anderes ergibt, vom Überwiegen der Geheimhaltungsinteressen auszugehen.

Abs. 1 regelt die generellen Erlaubnistatbestände großteils nach dem Muster der Richtlinie (mit Ausnahme des Art. 7 lit. e) – öffentliches Interesse, der im Hinblick auf Abs. 2 entbehrlich scheint).

(2) In Vollziehung der Gesetze dürfen Daten unter Einhaltung der Grundsätze des § 5 nur verarbeitet werden, wenn dafür eine ausdrückliche gesetzliche Ermächtigung besteht, oder soweit dies für den für die Verarbeitung Verantwortlichen zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bildet. Für die Einräumung eines Direktzugriffs auf eine Verarbeitung in der Weise, daß es im Belieben der zugreifenden Behörde oder Person steht, welche Daten sie abruft, ist jedenfalls eine ausdrückliche gesetzliche Ermächtigung notwendig.

Abs. 2 faßt gebündelt die Regelung für den „öffentlichen Bereich“ zusammen. In den Erläuterungen sollte darauf hingewiesen werden, daß dieser Absatz bei Übermittlungen jeweils auf jene Seite anzuwenden ist, für die die Übermittlung bzw. Ermittlung „in Vollziehung der Gesetze“ liegt. Demgegenüber erscheint die Formulierung in § 7 Abs. 2 des Entwurfs verfehlt, wenn bei Übermittlungen von *Auftraggebern des öffentlichen Bereichs auch geprüft wird, ob die Übermittlung für den* Empfänger *eine wesentliche Voraussetzung für den Vollzug einer ihm gesetzlich übertragenen Aufgabe bildet. Der Empfänger muß ja nicht zum*

(3) Bestehende gesetzliche Verschwiegenheitspflichten werden durch Abs. 1 und 2 nicht berührt.

(4) Für ausschließlich private, insbesonders familiäre Zwecke dürfen Daten unter Einhaltung der Grundsätze des § 5 dann verarbeitet werden, wenn sie dem für die Verarbeitung Verantwortlichen von der betroffenen Person selbst mitgeteilt wurden oder dem für die Verarbeitung Verantwortlichen als

Privatperson sonst rechtmäßigerweise zugekommen sind. Solche Daten dürfen nur mit Einwilligung der betroffenen Person übermittelt werden.

Abs. 4 faßt die im Entwurf auf zwei Absätze in verschiedenen Paragraphen verteilte Regelung der privaten Verarbeitung in einem Absatz zusammen.

(5) Nicht registrierte Übermittlungen sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 23 gegeben werden kann. In der Standardverordnung (§ 15 Abs. 4 Z 4) und in der Musterverordnung (§ 16 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

Die Sonderbestimmungen der §§ 41ff des Entwurfs sollten aus systematischen Gründen auch eher in diesem Bereich angesiedelt werden, da es sich ja im wesentlichen um spezielle Zulässigkeitstatbestände handelt. Siehe dazu die oben bei § 5 vorgeschlagene Gliederung.

§ 10 – Genehmigungsfreie Übermittlung und Überlassung von Daten ins Ausland

Wenn das Grundrecht auf Datenschutz weiterhin auch juristische Personen umfaßt, folgt als logische Konsequenz – da durch die Richtlinie nur der Datenschutz natürlicher Person vereinheitlicht wurde – daß die Übermittlung und Überlassung von Daten juristischer Personen ins Ausland einer Genehmigungspflicht unterzogen werden muß. Das führt dazu, daß Verarbeitungen mit Daten juristischer Personen „besser geschützt“ sind als die Daten natürlicher Personen, welche frei durch Europa transportiert werden dürfen. Auch aus diesem Grund plädiert die ARGE DATEN dafür, den Datenschutz für juristische Personen zu streichen.

Zu Abs. 5: Nicht bloß die Einhaltung der §§ 6 und 7, sondern auch die Einhaltung von § 5 (Datenqualität) muß Bedingung für die Zulässigkeit der Übermittlungen und Überlassungen in das Ausland sein.

§ 14 – Datenverarbeitungsregister

Die ARGE DATEN begrüßt, daß die Möglichkeit geschaffen werden soll, Eintragungen in das Datenverarbeitungsregister auf automationsunterstütztem Weg vorzunehmen. Dementsprechend sollte auch die Einsichtnahme in das Register auf elektronischem Weg (am zweckmäßigsten über das Internet) möglich sein.

§ 15 – Meldepflicht des Auftraggebers

Der vorgesehene § 15 Abs. 5 ermöglicht die Ausnahme mehrerer sensibler Datenverarbeitungen aus der Registrierungspflicht, ohne daß es dafür eine Notwendigkeit gäbe. Was „Datenverarbeitungen für Zwecke des Schutzes der verfassungsmäßigen Einrichtungen“ sein sollen, blieb seit 1978 (als diese Formulierung in § 4 Abs. 3 aufgenommen wurde) unklar. Ebenso bestand seit 1978 kein Bedarf, Datenverarbeitungen „für Zwecke der umfassenden Landesverteidigung“ von bestimmten Bestimmungen des DSG auszunehmen. Die Datenverarbeitungen „für Zwecke der Strafrechtspflege“ (das sind im wesentlichen Datenverarbeitungen der Polizei) und „für Zwecke der Sicherung der Einsatzbereitschaft des Bundesheeres“ sind äußerst sensible Verarbeitungen. Gerade diese sollten in einem demokratischen Staat dokumentiert und offengelegt werden. Es ist nicht einzusehen, wieso es für Polizei und Bundesheer ein Problem sein sollte, öffentlich zu dokumentieren, welche Arten von Daten von ihnen verarbeitet werden.

Angesichts der immer größeren Verbreitung von Datenbanken auf CD-ROM (z. B. Telefonbuch, TOP-500-Unternehmen samt Namen der Vorstandsmitglieder etc.), sollte man sich weitere Ausnahmen von der Registrierungspflicht überlegen. Derzeit ist jeder, der eine Telefonbuch-CD-ROM installiert, Auftraggeber im Sinne des DSG und müßte diese Datenverarbeitung registrieren lassen. Denkbar wäre hier eine Lösung, wonach der Produzent einer CD-ROM bei der DSK eine Art „Typengenehmigung“ für sein Produkt beantragen könnte, die seine Kunden von der Registrierungspflicht befreit. Dieses Genehmigungsverfahren würde der DSK auch die Möglichkeit geben, im Wege von Auflagen und Bedingungen datenschutzrechtliche Nachteile solcher Produkte abzumildern.

Dasselbe gilt für Produzenten von Software. Auf praktisch jedem neu verkauften Computer ist serienmäßig ein E-Mail-Programm installiert, das selbstverständlich über eine Adreßbuchfunktion verfügt, sowie über die Möglichkeit, gespeicherte E-Mails gezielt z. B. nach der Person des Absenders oder des Empfängers zu durchsuchen. Dies stellt zweifellos eine – an sich registrierungspflichtige – Datenverarbeitung dar. Da die technologische Entwicklung sehr rasch voranschreitet, wäre auch hier die relativ rasch bewilligbare Befreiung von der Registrierungspflicht durch eine „Typengenehmigung“ praktikabler als das schwerfällige Instrument der Verordnung.

§ 18 – Registrierung

Zu § 18 Abs. 2: Die Registrierung sollte (wie in einem früheren Entwurf überlegt) in Bescheidform erfolgen, damit dem Auftraggeber ein Rechtsmittel dagegen offen steht.

Wie bisher praktiziert, soll dem Auftraggeber die ihm zugeteilte Registernummer sofort bekanntgegeben werden und nicht erst mit Abschluß der Registrierung. Der Auftraggeber muß diese Nummer ja auf Formularen, Briefpapier oder dgl. anbringen und bei vielen EDV-Programmen eintragen und soll dazu möglichst früh in der Lage sein.

§ 21 – Informationspflicht

Der im Entwurf vorgesehene Text bleibt weit hinter dem zurück, was die Richtlinie vorschreibt. Zunächst sieht der Entwurf eine Ausnahme von der Informationspflicht für alle nicht meldepflichtigen Verarbeitungen vor (§ 21 Abs. 4), was der Richtlinie klar widerspricht. **Die Informationspflicht muß prinzipiell für alle Verarbeitungen gelten.**

Ausnahmen für Verarbeitungen zu persönlichen und familiären Zwecken sind in Ordnung, aber die große Masse der Standardverarbeitungen darf nicht pauschal ausgenommen werden: Entgegen der in den Erläuterungen zum Entwurf vertretenen Ansicht kann der Betroffene nämlich im Bundesgesetzblatt nur die Information ablesen, welche Standardverarbeitungen es gibt. Daß er in der Standardverarbeitung der Firma X oder der Bank Y registriert wurde, kann er aber nur erkennen, wenn X und Y verpflichtet sind, ihn darüber zu informieren. Genau das ist es, was die Richtlinie bezweckt.

Die Richtlinie sieht eine detaillierte Information des Betroffenen über die Empfänger der Daten, über die Frage, ob die Beantwortung der Fragen durch den Betroffenen obligatorisch ist und eine Belehrung über die Auskunfts- und Berichtigungsrechte vor.

Der Entwurf versucht dagegen, die Informationspflicht durch eine Anhäufung von Ausnahmen zu unterlaufen: „in geeigneter Weise“, „falls diese Information dem Betroffenen ... nicht bereits ... vorliegt“, „darf die Information ... entfallen, wenn ...“, „wenn dies nach der Übung des redlichen Verkehrs erforderlich ist“, „die Informationspflicht entfällt, wenn ...“

Der Entwurf ist weit davon entfernt, den Anforderungen der Richtlinie zu entsprechen. Daher sollte der Paragraph

grundlegend neu formuliert und möglichst stark am Text der Richtlinie (Art. 10 und 11) angelehnt werden.

§ 22 – Pflicht zur Offenlegung der Identität des Auftraggebers

In Abs. 1 wäre eine Aufzählung der geforderten Angaben (Name, Adresse, DVR-Nummer) sinnvoll.

Die ARGE DATEN begrüßt den vorgeschlagenen Abs. 2, der ein häufiges Problem der Praxis – Aufkleben von Adreßetiketten eines befreundeten Auftraggebers – für die Betroffenen durchschaubarer macht.

§ 23 – Auskunftsrecht

Bei modernen Datenverarbeitungen kann man immer schwerer zwischen den Daten und dem Programm unterscheiden. Objektorientiert programmierte Anwendungen bearbeiten *Objekte*, in denen *Daten* („Eigenschaften der Objekte“) und kleine *Programme* („Methoden der Objekte“) untrennbar verbunden werden. Was z. B. in einem Buchhaltungsprogramm früher einfach ein *Datensatz* war, der von Menschen mit Hilfe der EDV gelesen und bearbeitet wurde, kann nun als Objekt programmiert werden, das selbsttätig nach einer gewissen Frist ein Mahnschreiben verschickt und nach erfolglosem Verstreichen dieser Frist selbsttätig die Weiterleitung der Daten an den Rechtsanwalt veranlaßt.

Deshalb wird es für den Betroffenen immer wichtiger werden, nicht bloß zu erfahren, welche Daten in einem bestimmten Computersystem gespeichert sind, sondern auch, wie dieses System die Daten interpretiert und welche Aktionen es beim Vorliegen bestimmter Umstände automatisch setzen wird.

Dem trägt die Richtlinie Rechnung, indem sie auch eine Auskunftspflicht über die den „logischen Aufbau der automatisierten Verarbeitung“ vorsieht (Art. 12 lit. a dritter Gedankenstrich). Der Entwurf verabsäumt es, diesen wichtigen Aspekt aufzugreifen.

§ 25 – Widerspruchsrecht

a) Die ARGE DATEN begrüßt den Vorschlag des § 25 Abs. 2, der einen allgemeinen Anspruch auf Löschung aus öffentlichen Verzeichnissen (wie z. B. Telefonbücher) jenen Personen gewährt, die nicht darin eingetragen werden wollen.

b) **Der Entwurf setzt das von der Richtlinie vorgesehene Widerspruchsrecht gegen Datenverarbeitung für Zwecke der Direktwerbung nicht um.** Die in den Erläuterungen vertretene Auffassung, daß diese Bestimmung schon in § 268 Gewerbeordnung umgesetzt sei, ist falsch: § 268 GewO gilt nur für Adressenverlage und Direktwerbeunternehmen, das Widerspruchsrecht gemäß Art. 14 lit. b der Richtlinie jedoch für alle Datenverarbeiter.

§ 26 – Kontrollbefugnisse der Datenschutzkommission

Die im Entwurf genannten Kontrollbefugnisse sollten vom Bundesdatenschutzbeauftragten wahrgenommen werden. Dieser soll auch die Möglichkeit haben, gegenüber den für die Verarbeitung Verantwortlichen Empfehlungen und Aufforderungen auszusprechen, und Stellungnahmen im Registrierungsverfahren abgeben können. Der Bundesdatenschutzbeauftragte soll auch (entsprechend Art. 28 Abs. 3 zweiter Gedankenstrich der Richtlinie) für die geeignete Veröffentlichung seiner Stellungnahmen und Empfehlungen sorgen können.

Wenn den Empfehlungen nicht entsprochen wird, soll der Bundesdatenschutzbeauftragte die in § 26 Abs. 3 des Entwurfs angesprochenen Verfahren bei der DSK, einem Zivilgericht oder einer Strafverfolgungsbehörde einleiten können und in diesen Verfahren Parteistellung besitzen.

Die in § 26 Abs. 1 vorgesehene Möglichkeit, eine „Eingabe an die Datenschutzkommission“ zu machen, steht in einem gewissen Konflikt zur Beschwerde bei der Datenschutzkommission und zur Klage bei Gericht. Die DSK hat nämlich gemäß § 26 Abs. 2 (auch im privaten Bereich) die Eingabe verpflichtend zu prüfen und allenfalls „Empfehlungen“ auszusprechen, an deren Nichtbefolgung gewisse, wenn auch schwache Sanktionen geknüpft sind. Damit entsteht eine im Sinne der Gewaltentrennung bedenkliche Parallelität zwischen verwaltungsbehördlichem Verfahren bei der DSK und gerichtlichem Verfahren.

Auch aus diesem Grund wäre es sinnvoll, einen Bundesdatenschutzbeauftragten einzurichten, an den dann Eingaben gerichtet werden können, mit denen Verletzungen datenschutzrechtlicher Vorschriften aufgezeigt werden. Dabei soll es durchaus möglich sein, neben der Verletzung eigener Rechte auch die Verletzung der Datenschutzrechte anderer Personen anzuzeigen.

Im Sinne der von uns vorgeschlagenen Institutionenreform hätte dann ein Bürger mehrere Möglichkeiten: Wenn er in

einem rechtsförmlichen Verfahren eine verbindliche Entscheidung erzwingen will, wendet er sich an die DSK bzw. die Gerichte. (Das ist natürlich nur bei Verletzung eigener Rechte möglich.) Wenn er einen datenschutzrechtlichen Mißstand aufzeigen will, ohne daß er selbst an einer Parteistellung im Verfahren interessiert ist, kann er den Bundesdatenschutzbeauftragten informieren, welcher die Sache dann von Amts wegen verfolgt und bei Bedarf DSK-Beschwerde oder Klage bei Gericht ergreifen kann.

§ 26a – Rechtsschutz

Das Beschwerderecht bei der DSK und die Klagemöglichkeit bei Gericht sollen – wie in § 26 des Entwurfs richtig erkannt wurde **nicht bloß für Verletzungen des DSG gelten, sondern auch für Verletzungen der datenschutzrechtlichen Vorschriften anderer Mitgliedstaaten der EU.** (Gemäß dem Sitzstaatprinzip der Richtlinie – § 2 des Entwurfs – ist z. B. französisches Datenschutzrecht anzuwenden, wenn der Auftraggeber seinen Sitz in Frankreich hat und die Verarbeitung keiner Niederlassung in Österreich zuzurechnen ist.) Es ist angesichts der immer stärkeren europäischen Vernetzung nicht undenkbar, daß auch ein ausländischer Rechtsträger in Österreich in Vollziehung der Gesetze tätig wird und damit unter die Zuständigkeit der DSK fällt.

Um nicht an mehreren Stellen auf „dieses Bundesgesetz“ und „datenschutzrechtliche Vorschriften eines anderen Mitgliedstaates ...“ verweisen zu müssen, schlagen wir die Einfügung eines Paragraphen vor, in dem alle Beschwerdemöglichkeiten aufgezählt sind:

> § 26a. (1) Ansprüche wegen Verletzung der Rechte nach diesem Bundesgesetz oder nach datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates der Europäischen Union, die gemäß § 2 im Inland Anwendung finden, sind
> 1. mit Beschwerde an die Datenschutzkommission (§ 27) geltend zu machen, wenn sie sich gegen einen Rechtsträger des öffentlichen Rechts oder einen in Vollziehung der Gesetze tätigen Rechtsträger des Privatrechts richten und das verletzende Verhalten nicht ein Akt der Gerichtsbarkeit oder der Gesetzgebung ist;
> 2. auf dem ordentlichen Rechtsweg (§ 28) geltend zu machen, wenn sie sich gegen einen nicht in Vollziehung der Gesetze tätigen Rechtsträger des Privatrechts richten;
> 3. mit Beschwerde an den organisatorisch übergeordneten Gerichtshof (§ 28a) geltend zu machen, wenn das verletzende Verhalten ein Akt der Gerichtsbarkeit ist.
>
> (2) Schadenersatzansprüche sind jedenfalls auf dem ordentlichen Rechtsweg geltend zu machen.

Wie unter A. 7. ausgeführt ist die eindeutige Trennung in „Auftraggeber des öffentlichen Bereichs“ und „Auftraggeber des privaten Bereichs“ aufgrund der vom Entwurf beibehaltenen

unglücklichen Formulierung des § 1 Abs. 6 DSG verfassungsrechtlich nicht möglich. Da das Grundrecht auf Datenschutz bei Rechtsträgern, die in Formen des Privatrechts eingerichtet sind (z. B. Telekom-Control-GmbH, AMS), soweit sie nicht in Vollziehung der Gesetze tätig werden, im Zivilrechtsweg geltend zu machen ist, wäre es (zwar wünschenswert aber) verfassungswidrig, z. B. für die Telekom-Control-GmbH generell die Datenschutzkommission zuständig zu machen.

Wie unter A. 5. ausgeführt, sollte für das Auskunftsrecht nicht eine andere Behörde zuständig sein als für alle anderen Betroffenenrechte gegenüber demselben Auftraggeber.

Ob es verfassungsrechtlich vom Grundsatz der Gewaltenteilung wirklich geboten ist, Akte der Gesetzgebung (z. B. des Rechnungshofs!) aus dem Zuständigkeitsbereich der DSK auszunehmen, sollte noch untersucht werden. Art. 94 B-VG gebietet ja nur eine Trennung von Justiz und Verwaltung, nicht eine Trennung von Gesetzgebung und Verwaltung.

§ 27 – Beschwerde an die Datenschutzkommission

Anstelle der Absätze 1 und 2 des Entwurfs schlagen wir den oben genannten § 26a vor. Siehe dazu die Ausführungen oben.

§ 28 – Anrufung der Gerichte

Für Klagen auf Feststellung, Beseitigung und Unterlassung sollte das Bezirksgericht sachlich zuständig sein, wobei ein niedriger fiktiver Streitwert festgesetzt werden sollte, damit die Klage nicht dem Anwaltszwang unterliegt.

Für Schadenersatzklagen sollte nach den allgemeinen Grundsätzen je nach Höhe des Streitwerts (Schadens) das Bezirks- oder Landesgericht sachlich zuständig sein.

Anstelle der im Entwurf in Abs. 4 vorgesehenen Möglichkeit der Feststellungsklage der Datenschutzkommission sollte der Bundesdatenschutzbeauftragte die Möglichkeit haben, nicht nur auf Feststellung, sondern (wie ein Betroffener) auch auf Unterlassung und Beseitigung des den datenschutzrechtlichen Vorschriften widersprechenden Zustands zu klagen. Der Bundesdatenschutzbeauftragte sollte auch (statt der DSK) einem Rechtsstreit als Nebenintervenient beitreten können (Abs. 5).

Textvorschlag (siehe auch das in A. 5. zur Institutionenreform und unter A. 7. zur Trennung von öffentlichem und privatem Bereich Gesagte):

§ 28 (1) Sind Daten entgegen der datenschutzrechtlichen Vorschriften verarbeitet worden, so hat die betroffene Person Anspruch auf Unterlassung und Beseitigung des den datenschutzrechtlichen Vorschriften widerstreitenden Zustandes.

(2) Für Klagen nach Abs. 1 ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Bezirksgericht zuständig, in dessen Sprengel die betroffene Person ihren gewöhnlichen Aufenthalt oder Sitz hat. Klagen können aber auch bei dem Bezirksgericht erhoben werden, in dessen Sprengel der für die Verarbeitung Verantwortliche seinen gewöhnlichen Aufenthalt oder Sitz hat.

(3) Der Bundesdatenschutzbeauftragte kann in Fällen, in welchen er schwerwiegende Datenschutzverletzungen vermutet, eine Feststellungsklage (§ 228 ZPO) oder eine Klage auf Unterlassung oder Beseitigung des den datenschutzrechtlichen Vorschriften widerstreitenden Zustandes erheben. Zuständig ist in erster Instanz jenes Bezirksgericht, in dessen Sprengel der für die Verarbeitung Verantwortliche seinen gewöhnlichen Aufenthalt oder Sitz hat. Hat der für die Verarbeitung Verantwortliche keinen gewöhnlichen Aufenthalt oder Sitz in Österreich, dann ist das Bezirksgericht Innere Stadt Wien zuständig.

(4) Der Bundesdatenschutzbeauftragte kann, wenn eine betroffene Person es verlangt und es zur Wahrung der datenschutzrechtlichen Interessen einer größeren Zahl von betroffenen Personen geboten ist, einem Rechtsstreit auf Seiten der betroffenen Person als Nebenintervenient (§§ 17ff ZPO) beitreten.

§ 28a – Beschwerde gegen ein Gericht

Noch ungeregelt ist die Zuständigkeit für Beschwerden gegen Datenschutzverletzungen durch die Gerichtsbarkeit. Wir schlagen dafür die Möglichkeit einer Beschwerde an das organisatorisch übergeordnete Gericht (Alternative: an den OGH) vor. Die entsprechenden Bestimmungen sollten sich an die DSK-Beschwerde bzw. an die Grundrechtsbeschwerde beim OGH anlehnen.

Textvorschlag:

Beschwerde gegen ein Gericht

§ 28a. (1) Über Beschwerden gegen die Verletzung von Datenschutzrechten durch ein Bezirksgericht, einen Gerichtshof erster Instanz bzw. einen Gerichtshof zweiter Instanz entscheidet jeweils der organisatorisch übergeordnete Gerichtshof erster Instanz, Gerichtshof zweiter Instanz bzw. der Oberste Gerichtshof.

(2) Die Beschwerde ist bei dem Gericht einzubringen, das über die Beschwerde zu entscheiden hat, und hat das verletzende Verhalten oder die angefochtene Entscheidung oder Verfügung zu bezeichnen.

(3) Über die Beschwerde ist in nichtöffentlicher Sitzung in einem Senat von drei Richtern durch Beschluß (vom Obersten Gerichtshof durch Erkenntnis) zu entscheiden.

(4) In der Entscheidung ist auszusprechen, ob eine Verletzung der Datenschutzrechte stattgefunden hat, und erforderlichenfalls die angefochtene Entscheidung oder Verfügung aufzuheben.

(5) Wird der Beschwerde stattgegeben, so ist das belangte Gericht verpflichtet, mit den ihm zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung des entscheidenden Gerichtes entsprechenden Rechtszustand herzustellen.

In der Vollzugsklausel wäre der Bundesminister für Justiz mit der Vollziehung dieses Paragraphen zu betrauen.

§ 29 – Schadenersatz

§ 29 (5) Die örtliche Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 28 Abs. 2, die sachliche Zuständigkeit nach dem Wert des Streitgegenstandes (§ 49 Abs. 1 JN).

§ 30 – Datenschutzkommission und Datenschutzrat

Diese Bestimmung dürfte (wie die Vorgängerbestimmung § 35 Abs. 1 DSG) keinen eigenständigen normativen Gehalt haben und kann daher entfallen. Es genügt die Vollzugsklausel des § 54.

§ 31 – Aufgaben der Datenschutzkommission

Entsprechend der in A. 5. vorgeschlagenen Institutionenreform und dem unter A. 7. zur Trennung von öffentlichem und privatem Bereich gesagtem, schlagen wir folgende Formulierung für § 31 Abs. 1 vor:

§ 31 (1) (Verfassungsbestimmung) Die Datenschutzkommission entscheidet:
1. über Beschwerden von Personen, die behaupten, in ihren Datenschutzrechten verletzt worden zu sein, soweit das verletzende Verhalten einem Rechtsträger des öffentlichen Rechts oder einem in Vollziehung der Gesetze tätigen Rechtsträger des privaten Rechts zuzurechnen ist und soweit dieses Verhalten nicht ein Akt der Gerichtsbarkeit oder der Gesetzgebung ist;
2. in Verfahren im Zusammenhang mit der Eintragung in das Datenverarbeitungsregister;
3. über die Erteilung einer Genehmigung für den internationalen Datenverkehr.

Z. 1 (Auskunftserteilung) wurde gestrichen, ebenso Z. 3 (Bestreitungsvermerk), weil dieser Punkt unter den Oberbegriff „Verletzung von Rechten nach diesem Bundesgesetz“ subsumiert werden kann.

Die Überprüfung des Registers von Amts wegen (Abs. 2) sollte in die Zuständigkeit des Bundesdatenschutzbeauftragten fallen, der dann ein entsprechendes Verfahren bei der DSK einleiten könnte, in dem er als „Ankläger“ auftritt.

In die Zuständigkeit des Bundesdatenschutzbeauftragten sollte auch die in Abs. 3 und Abs. 5 genannte Kontrolltätigkeit fallen.

Das Anhörungsrecht vor der Erlassung von Verordnungen könnte allen Datenschutzinstitutionen (DSK, DSR, Bundesdatenschutzbeauftragter) gewährt werden.

§ 33 – Weisungsfreiheit der Mitglieder der DSK und Verschwiegenheitspflicht

Die in Abs. 2 verfassungsgesetzlich vorgeschriebene Verpflichtung zur Amtsverschwiegenheit kann entfallen, da die Mitglieder der DSK als mit Aufgaben der Bundesverwaltung betraute Organe ohnehin gemäß Art. 23 B-VG der Amtsverschwiegenheit unterliegen.

§ 41 – Sensible Daten

Völlig verfehlt ist die in § 41 als Verfassungsbestimmung (!) vorgeschlagene Regelung der Verarbeitung sensibler Daten.

Die Richtlinie sieht in Art. 8 ein prinzipielles Verarbeitungsverbot für sensible Daten („Die Mitgliedstaaten untersagen die Verarbeitung ...“) und einen begrenzten Katalog von Ausnahmen vor. Dies wurde auch richtigerweise in den Entwurf des Grundrechts (§ 1 Abs. 3 des Entwurfs: „unzulässig ... zur Wahrung wichtiger öffentlicher Interessen notwendig ... angemessene Garantien“) aufgenommen.

Demgegenüber enthält § 41 kein Verarbeitungsverbot, sondern nur Erlaubnistatbestände: „Sensible Daten natürlicher Personen dürfen jedenfalls verwendet werden, wenn dies ...“. Selbstverständlich wäre diese Bestimmung im Lichte des § 1 Abs. 3 des Entwurfs verfassungswidrig, wenn sie nicht selbst eine Verfassungsbestimmung wäre.

Um die Richtlinie korrekt umzusetzen, kann nicht ein Paragraph betreffend die Verarbeitung sensibler Daten neben die übrigen Erlaubnistatbestände der §§ 6 und 7 DSG gestellt werden. Es muß vielmehr das prinzipielle Verarbeitungsverbot sensibler Daten diese Erlaubnistatbestände überlagern.

Bei der Umsetzung des Art. 8 der Richtlinie wird man im Text des DSG auch nicht einfach auf „gesetzliche Ermächtigungen oder Verpflichtungen“ verweisen können, wie dies derzeit in § 6 Abs. 1 des Entwurfs gemacht wird. Vielmehr wird man die derzeit in den verschiedenen Gesetzen verstreuten

Ermächtigungen zur Datenverarbeitung daraufhin durchforsten müssen, ob allenfalls der Richtlinie widersprechende Datenverarbeitungen zu beseitigen sind. Dabei wäre insbesondere das Meldegesetz zu überprüfen, das bekanntlich eine Verarbeitung des Religionsbekenntnisses durch staatliche Behörden vorsieht, ohne daß dies durch Art. 8 Abs. 2 der Richtlinie gedeckt wäre.

§ 42 – Daten über Verurteilungen

Die ARGE DATEN begrüßt diese Bestimmung, die Datenverarbeitungen über Straftaten, strafrechtliche Verurteilungen oder vorbeugende Maßnahmen einer strengen Gesetzesbindung unterstellt.

§ 45 – Automatisierte Einzelentscheidungen

Angesichts der detaillierten Regelung in Art. 15 der Richtlinie erscheint der knapp gehaltene Vorschlag für § 45 Abs. 1 nicht als geeignet, die Richtlinie korrekt umzusetzen.

Die ARGE DATEN begrüßt den vorgeschlagenen Abs. 2, nach dem der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form dargelegt werden muß.

§ 46 – Informationsverbundsysteme

Die ARGE DATEN begrüßt den Vorschlag, daß bei Informationsverbundsystemen ein Betreiber bestimmt werden muß, der die Auftraggeberpflichten gegenüber den Betroffenen wahrnimmt. Damit wird das fachliche Know-how an einer Stelle gebündelt, was hoffentlich zu einer Verbesserung der datenschutzrechtlichen Situation in diesem Bereich führt.

§ 47 – Datenbeschaffung in Schädigungsabsicht

Nicht die Datenschutzkommission als unabhängige Behörde sondern der Bundesdatenschutzbeauftragte als „Datenschutzanwalt“ sollte den Antrag auf Verfolgung des Täters stellen können.

§ 48 – Verwaltungsstrafbestimmung

Zu Abs. 4: Das in diesem Absatz zitierte Verwaltungsstrafgesetz 1950 wurde 1991 wiederverlautbart und heißt seither „Verwaltungsstrafgesetz 1991 – VStG“.

§ 52 – Inkrafttreten

Aufgrund der Vorgaben der Richtlinie ist zu wünschen, daß das neue DSG bereits vor dem 1. Jänner 1999 (nämlich vor dem 24. Oktober 1998) in Kraft tritt.