AMT DER NIEDERÖSTERREICHISCHEN LANDESREGIERUNG
Gruppe Landesamtsdirektion - Abteilung Landesamtsdirektion/Verfassungsdienst

Kennzeichen
LAD1-VD-00401/2

Frist

DVR: 0059986

Bezug

Bearbeiter (0 27 42) 200
Mag. Heißenberger

Durchwahl
2095

Datum
24. Juli 2000

Betrifft
NÖ Datenschutzgesetz (NÖ DSG); Motivenbericht

Landtag von Niederösterreich
Landtagsdirektion
Eing.: - 6. JULI 2000
Ltg. 499/D-3
V- Aussch.

Hoher Landtag!

Zum Gesetzesentwurf wird berichtet:

Allgemeiner Teil

1. Beschreibung des Ist-Zustandes:

Am 24. Oktober 1995 wurde die "**Richtlinie 95/46/EG** des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" verabschiedet. Art. 32 Abs. 1 dieser Richtlinie gibt den Mitgliedsstaaten eine dreijährige Frist zur Umsetzung der Richtlinie in das innerstaatliche Recht. Für Österreich besteht daher insofern akuter Umsetzungsbedarf, als einige inhaltliche Erfordernisse der Richtlinie 95/46/EG im geltenden DSG, BGBl. Nr. 565/1978 in der geltenden Fassung, nicht vollständig oder in etwas anderer Ausprägung enthalten sind.

Ziel der Richtlinie ist die **Harmonisierung der Datenschutzvorschriften** der Mitgliedstaaten der Europäischen Union. Dies ist die Voraussetzung dafür, dass in Hinkunft kein Mitgliedstaat mehr den grenzüberschreitenden Datenverkehr innerhalb des EU-Gebiets im Interesse des Datenschutzes besonderen Prüfungen oder Genehmigungen unterwerfen darf. Das EU-Gebiet soll auch im Hinblick auf die Kommunikation personenbezogener Daten ein Raum sein, in dem der freie Verkehr von Daten im Hinblick auf das Funktionieren des Binnenmarktes durch nationale Grenzen nicht behindert wird bei gleichzeitiger Wahrung des Schutzes der Grundrechte (vgl. hiezu auch Damann/Simitis, EG-Datenschutzrichtlinie-Kommentar, 1997, S. 65).

2. Beschreibung des Soll-Zustandes:

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

und zum freien Datenverkehr ist bereits durch das derzeit in Österreich geltende Datenschutzgesetz weitest gehend umgesetzt. Um ein Maximum an Harmonisierung zu erreichen hat der Bund in Umsetzung der Richtlinie 95/46/EG ein neues Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl. I Nr. 165, erlassen. Durch dieses Gesetz wird die Richtlinie 95/46/EG mit kleineren Ausnahmen, die sich aus der föderalistischen Struktur Österreichs ergeben und lediglich bestimmte manuelle Dateien betreffen, umgesetzt. Dieses Gesetz tritt am 1. Jänner 2000 in Kraft. Da entsprechend der Kompetenzverteilung für manuell strukturierte Daten der Landesgesetzgeber zuständig ist, ist im Hinblick auf ein in der Zwischenzeit eingeleitetes Vertragsverletzungsverfahren gegen die Republik Österreich Handlungsbedarf betreffend die Umsetzung der Richtlinie 95/46/EG gegeben.

Die **Betroffenenrechte,** die schon bisher im Grundrecht gegenüber automationsunterstützter Verwendung von Daten garantiert waren, wurden nunmehr **auf die Verwendung von Daten in manueller, strukturierter Form (z.B. in Karteien, Listen usw.) ausgedehnt,** wie es die Richtlinie verlangt.
In Umsetzung der Richtlinie 95/46/EG ist Betroffener nur eine natürliche Person.

Die **Zulässigkeitsvoraussetzungen** für die Ermittlung, Verarbeitung und Übermittlung von Daten waren neu zu formulieren, und zwar zum Ersten deshalb, weil öffentlicher und privater Bereich nunmehr zusammengefasst sind, und zum anderen, weil die Artikel 6, 7 und 8 der Richtlinie 95/46/EG entsprechend zu berücksichtigen waren. Wie in der Richtlinie vorgezeichnet, wird den Bestimmungen über die Zulässigkeit der Datenverwendung ein Katalog von **"Grundsätzen"** vorangestellt, der die obersten Prinzipien rechtmäßigen Umgangs mit personenbezogenen Daten enthält.

Als **unabhängige Kontrollstelle im Sinne des Art. 28** der Richtlinie 95/46/EG wird die Datenschutzkommission eingesetzt, der die Kontrolle über sämtliche Auftraggeber von Datenanwendungen – soweit sie nicht der Gerichtsbarkeit oder der Gesetzgebung zuzurechnen sind – als zusätzliche, neue Kompetenz übertragen wird.

Die im Begutachtungsverfahren abgegebene Stellungnahmen und Anregungen wurden weitgehend berücksichtigt.

3. Darstellung der Kompetenzlage:

Der vorliegende Entwurf wurde auf Grundlage der geltenden Kompetenzverteilung erstellt. Er kann daher die Richtlinie 95/46/EG nur insoweit umsetzen, als hiefür eine Gesetzgebungskompetenz des Landes besteht.

Beim Datenschutz handelt es sich grundsätzlich um eine Annexmaterie. Gemäß der Verfassungsbestimmung des Art. 1 des Datenschutzgesetzes 2000 – DSG 2000 ist Bundessache die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr. Daraus folgt, dass der Bund für automationsunterstützten Datenverkehr eine Kompetenzgrundlage im § 2 des Art. 1 des Datenschutzgesetzes 2000 – DSG 2000 geschaffen hat. Daher ist davon auszugehen, dass für die manuell strukturierten Daten (Handkarteien) eine Kompetenz des Landesgesetzgebers besteht. Dies betrifft jedoch nur jene Rechtsmaterien, die nach der allgemeinen Kompetenzverteilung (insbesondere Art. 15 B-VG) in die Kompetenz des Landes fallen. Jene manuelle Dateien, die ohne Automationsunterstützung für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenanwendung im Sinne des § 4 Z. 7 DSG 2000 (vgl. § 58 Datenschutzgesetz 2000 – DSG 2000, BGBl. I Nr. 165/1999).

4. Verhältnis zu anderen landesrechtlichen Vorschriften:

Aus dem NÖ Datenschutzgesetz kann keine unmittelbare Verpflichtung zur Harmonisierung der Materiengesetze mit dem NÖ Datenschutzgesetz abgeleitet werden, da vielmehr sogar Hinweise (z.B. § 7 Zulässigkeit der Verwendung von Daten) auf die einzelnen Materiengesetze im NÖ Datenschutzgesetz erfolgen.

Der Gleichklang wird jedoch im Hinblick, dass das NÖ Datenschutzgesetz in Ausführung der Richtlinie 95/46/EG und des Grundrechtes erfolgt, anzustreben sein.

5. Klimabündnis:

Der vorliegende Entwurf hat keine Auswirkungen auf die Erreichung der im Klimabündnis vorgesehenen Ziele.

6. Beschreibung der finanziellen Auswirkungen:

Gemäß Art. 6 Abs. 1 Z. 1 **gilt die Vereinbarung** zwischen dem Bund, den Ländern und den Gemeinden über einen **Konsultationsmechanismus** und einen künftigen Stabilitätspakt der Gebietskörperschaften **nicht** für rechtsetzende Maßnahmen, die eine Gebietskörperschaft aufgrund zwingender Maßnahmen des Gemeinschaftsrechts zu setzen verpflichtet ist (LGBl. 0814-0).

Was die **Vorabkontrolle bei manuellen Datenanwendungen** (vgl. § 18) betrifft, kann er nur dort überhaupt ins Gewicht fallen, wo traditionellerweise umfangreiche personenbezogene Dateien mit **sensiblen Daten** gehalten werden: Dies wäre etwa bei Ärzten und

ähnlichen Berufszweigen der Fall. Da jedoch auch in diesen Bereichen die Patientenverwaltung zunehmend mit Hilfe der EDV vorgenommen wird, werden in naher Zukunft immer weniger Fälle von dieser besonderen neuen Vorabkontrolle betroffen sein. Dass diese Vorabkontrolle sachlich sinnvoll ist, ergibt sich daraus, dass dadurch verhindert werden kann, dass besonders sensible Informationen zur Umgehung der Transparenzpflichten des Datenschutzes in Form von manuellen Karteien oder Listen gespeichert werden.

Der Aufwand für den Normadressaten ist folgendermaßen darzustellen:

Zur Ausdehnung der Auskunfts-, Richtigstellungs- und Löschungspflicht auf manuelle Dateien ist anzumerken, dass sich daraus wahrscheinlich keine hohen Mehrkosten ergeben werden, weil die Anzahl der dem Datenschutzgesetz unterliegenden manuellen Dateien nicht besonders groß sein wird (- Dateien für den privaten Gebrauch unterliegen der Pflicht zur Auskunftserteilung, Richtigstellung und Löschung nicht -) und weil die Ausübung dieser Rechte des Betroffenen auch bei den automationsunterstützt geführten Dateien in den letzten 20 Jahren seit Inkrafttreten des Datenschutzgesetzes keine bedeutenden Kosten verursacht hat. Kosten für den Normadressaten könnten sich ergeben, beim im Gesetz geregelten Verfahren zur Vorabkontrolle (vgl. § 18), bei der Daten die der Vorabkontrolle unterliegen, der Datenschutzkommission mitzuteilen sind. Es ist davon auszugehen, dass für die Mitteilung dieser Daten ein Zeitaufwand von ca. einer Stunde erforderlich sein wird. Bei Heranziehung des Kostenersatzes könnte das Gerichtsgebührenanspruchsgesetz 1975 verwendet werden. Als Entschädigung wird für Zeitversäumnis S 167,-- für jede wenn auch nur begonnene Stunde angesetzt.

7. Probleme bei der Vollziehung:

Da das NÖ Datenschutzgesetz neu erlassen wird, kann zum jetzigen Zeitpunkt keine Aussage über Probleme bei der Vollziehung erfolgen.

8. Mitwirkung von Bundesorganen:

Gemäß der Verfassungsbestimmung des § 1 Abs. 5 DSG 2000 obliegt die Entscheidung über Verletzungen des Grundrechts auf Auskunft sowie sonstige Verletzungen des Grundrechts auf Datenschutz durch Auftraggeber des öffentlichen Bereichs der Datenschutzkommission. In diesem Bereich steht die Verfassungsbestimmung des § 1 Abs. 5 DSG 2000 der Betrauung einer anderen Behörde als der Datenschutzkommission entgegen. Insoweit im 7. Abschnitt des NÖ Datenschutzgesetzes darüber hinaus gehende Befugnisse der Datenschutzkommission übertragen werden, ist eine Zustimmung gemäß Art. 97 Abs. 2 B-VG erforderlich.

Besonderer Teil

1. Zu § 1:

Die Umsetzung der Richtlinie 95/46/EG in diesem Gesetz bezieht sich lediglich auf den Schutz personenbezogener Daten im **nicht automationsunterstützt** geführten **Datenverkehr**. Für automationsunterstützte Daten ist eine Kompetenz des Bundesgesetzgebers im Datenschutzgesetz 2000 vorgesehen. Abs. 2 stellt klar, dass nur jene manuelle Dateien vom Gesetz umfasst sind, die für Zwecke angelegt und benützt werden, die eine Angelegenheit der Landesgesetzgebungskompetenz darstellt. Manuelle Dateien, die in Angelegenheiten geführt werden, für die die **Bundesgesetzgebungskompetenz** besteht, werden vom vorliegenden Gesetzesentwurf **nicht umfasst**.

2. Zu § 2:

Diese Bestimmung definiert den Geltungsbereich des Gesetzes in räumlicher Hinsicht. Diese Bestimmung lehnt sich an § 3 des Datenschutzgesetzes 2000 an, trägt jedoch dem Umstand Rechnung, dass der Geltungsbereich einer Landesrechtsordnung auf das jeweilige Territorium des Landes beschränkt ist. Ausnahmen bestehen zu Gunsten des Sitzstaatsprinzips, das im Gemeinschaftsrecht angesichts der Dienstleistungsfreiheit eine gerne verwendete Kollisionsregel darstellt. Und zwar gilt diese Ausnahme zu Gunsten des Sitzstaatsprinzips dann, wenn Daten in Niederösterreich für einen Auftraggeber aus einem anderen EU-Staat verarbeitet werden, ohne dass der Auftraggeber (der seinen Sitz in einem anderen EU-Staat hat) eine feste Betriebsstätte in Niederösterreich hätte. Umgekehrt gilt niederösterreichisches Datenschutzrecht in einem anderen EU-Staat dann, wenn ein niederösterreichischer Rechtsträger Datenverarbeitung im EU-Ausland betreibt, ohne dass dafür die Verfolgung seiner Interessen dort eine „Niederlassung" (vgl. dazu § 3 Z. 17) besitzt. Während der Ort der Niederlassung des Auftraggebers der maßgebliche Anknüpfungspunkt für die Frage des anwendbaren Rechts ist, soweit es sich um Datenanwendungen für einen Rechtsträger mit Sitz in einem EU-Mitgliedstaat handelt, gilt bei Datenanwendungen für Zwecke eines Rechtsträgers der keinen Sitz in einem EU-Mitgliedstaat hat, immer der Ort der Datenverwendung als Anknüpfungspunkt für die Anwendbarkeit einer nationalen Rechtsordnung (Art. 4 Abs. 1 lit. c der Richtlinie).

3. Zu § 3:

Zu Z. 1:

Die Richtlinie geht davon aus, dass Daten nicht nur dann "personenbezogen" sind, wenn die Identität des Betroffenen **für den** jeweiligen **Verwender** bestimmbar ist, sondern auch dann, wenn sie nur für einen Dritten (z.B. den Inhaber des Entschlüsselungscodes bei codierten Identitätsdaten) bestimmbar sind.

Zu Z. 2:

Um hier im Hinblick auf das Schutzinteresse eine sinnvolle Abstufung vornehmen zu können, wurde die in der Richtlinie enthaltene Unterscheidung zwischen direkter und (nur) indirekter Identifizierbarkeit nutzbar gemacht; wenn es für den konkreten Verwender der Daten nicht möglich ist, den – z.B. in Form einer laufenden oder sprechenden Nummer – vorhandenen Personenbezug auf eine in ihrer Identität bestimmte Person zurückzuführen, dann ist der Gebrauch solcher "nur indirekt personenbezogener" Daten durch **diesen** Verwender unter erleichterten datenschutzrechtlichen Bedingungen erlaubt.

Von den "nur indirekt personenbezogenen" Daten zu unterscheiden sind die üblicherweise als "anonymisiert" bezeichneten Daten. Bei anonymisierten Daten gibt es keinen Personenbezug; hiebei handelt es sich um Daten, die **niemand** auf eine in ihrer Identität bestimmte Person zurückführen kann. Derartige Daten sind daher auch nicht datenschutzrelevant.

Zu Z. 3:

Die Aufzählung der "sensiblen Daten" in **Z. 3** erfolgt in Umsetzung des Art. 8 Abs. 1 Richtlinie. Diese Aufzählung darf angesichts des taxativen Charakters des Art. 8 Abs. 1 Richtlinie weder erweitert noch verkürzt werden.

Zu Z. 4:

Diese Definition entspricht Art. 1 der Richtlinie 95/46/EG, der vorsieht, dass der Schutz der Privatsphäre **natürlicher Personen** bei der Verarbeitung personenbezogener Daten zu gewährleisten ist. Der Schutz von juristischen Personen ist von § 1 des DSG 2000 (Grundrecht auf Datenschutz) abgedeckt.

Zu Z. 5 und 6:

Die Ausdehnung der Definitionen von "Auftraggeber" und "Dienstleister" **(Z. 5 und 6)** auch auf Personengemeinschaften und auch auf Geschäftsapparate von Organen von Gebietskörperschaften (z.B. Bundesministerien, Ämter der Landesregierungen, usw.) dient der Angleichung an das DSG 2000. Gemäß Art. 2 lit. e der Richtlinie 95/46/EG ist somit auch „jede andere Stelle" mit umfasst.

Die genaue Regelung, wann ein Auftragnehmer als Auftraggeber gilt, dient dazu, Probleme in der Praxis hintanzuhalten. Die Betroffenenrechte kommen gegenüber jenen Personen zum Tragen, die dieser Rolle auch wirklich gerecht werden können; dies wird besonders deutlich, wenn es etwa um die Frage geht, an wen ein Auskunftsbegehren zu stellen ist.

An den Auftragnehmer kann der Betroffene sich deshalb nicht wenden, weil ihm seine Identität in aller Regel unbekannt sein wird. Ähnliches gilt für Löschungs- und Richtigstellungsansprüche: Die Erledigung eines solchen Anspruchs setzt die Verfügungsgewalt über die davon betroffenen Daten voraus, also eine Befugnis, die einem Auftragnehmer aus eigenem nicht zusteht. Auch im Interesse der Ausübbarkeit der Betroffenenrechte muss daher der vorgeschlagene Lösungsansatz als zweckmäßig erscheinen.

Nun gibt es jedoch einzelne Fälle von Beauftragungsverhältnissen, in welchen traditionellerweise der Beauftragte selbständig ("eigenverantwortlich") über die Verwendung der ihm übergebenen Informationen entscheidet und hiezu auch nach den für ihn geltenden Standesregeln verpflichtet und hiefür verantwortlich ist – dies gilt etwa für bestimmte freie Berufe, wie Rechtsanwälte, Wirtschaftstreuhänder, Ziviltechniker usw. Die Zuordnung der datenschutzrechtlichen Verantwortlichkeit eines Auftraggebers muss auf diese Besonderheiten Rücksicht nehmen. Um diesbezüglich die notwendige Rechtssicherheit herzustellen, wird es sich empfehlen, in Verhaltensregeln gemäß § 5 Abs. 2 klarzustellen, wem in gewissen Konstellationen die Auftraggebereigenschaft zukommt. Um für einen entsprechenden Schutz der Betroffenenrechte auch in diesen Fällen vorzusorgen, wurde die besondere Auskunftsverpflichtung § 17 geschaffen.

Zu Z. 7:

In der bei der Erarbeitung der Richtlinie stattgefundenen Diskussion wurde immer wieder betont, dass unter "Datei" bei der manuellen Verwendung von Daten keinesfalls ein Aktenkonvolut zu verstehen sei, sondern vielmehr Karteien, Listen u. dgl. Dieses gemeinsame Begriffsverständnis findet bedauerlicherweise im Definitionswortlaut nur ungenügenden Ausdruck: Um der kollektiven Absicht zu entsprechen, hätte es wohl eher heißen müssen, dass eine "Datei" eine **Sammlung strukturierter Datensätze** sei, die – nämlich die Sammlung – nach mindestens einem Suchkriterium geordnet ist. Eine historisch-teleologisch berichtigende Interpretation des tatsächlichen Textes scheint vor diesem Hintergrund nicht ausgeschlossen.

Zu Z. 8:

Der Begriff der "Datenanwendung" in der **Z. 8** entspricht im Prinzip dem bisherigen Begriff der "Datenverarbeitung" gemäß § 3 Z. 5 des geltenden DSG. Der neue Begriff "Datenanwendung" wurde nur gewählt, um eine bessere Unterscheidbarkeit zum Begriff des "Verarbeitens" von Daten (Z. 12) zu bewirken.

Wesentlich für das Begriffsinstrumentarium des Entwurfes ist jedenfalls, dass die "Datenanwendung" – so wie bisher die "Datenverarbeitung" – eine **logische** Einheit ist, die unterschiedlichste Handlungen umfasst, wie etwa das Verarbeiten **(Z. 12),** Übermitteln **(Z. 15),** usw. Das verbindende Element ist der Gesamtzweck der Datenanwendung, zu dessen Erreichung die einzelnen Schritte gesetzt werden.

Zu Z. 9 und 10:

Die Abgrenzung zwischen Auftraggebern des öffentlichen Bereichs und solchen des privaten Bereichs stellt darauf ab, nach welchem Rechtsregime der Auftraggeber **eingerichtet** ist. Eine gewisse **Korrektur** erfährt dieses Abgrenzungskriterium nur dort, wo Rechtsträger des privaten Rechts ausnahmsweise Hoheitsverwaltung betreiben, ein Fall, der angesichts der steigenden Anzahl von **Ausgliederungen** von Verwaltungsbereichen besonders zu berücksichtigen war. Die Wendung "in Vollziehung der Gesetze" ist im Sinne des Art. 23 B-VG so zu verstehen, dass auch die schlichte Hoheitsverwaltung mitumfasst ist.

Zu Z. 11:

Der umfassendste Begriff für die Handhabung von Daten ist der Begriff "Verwenden", der in **Z. 11** definiert wird. Der Begriff des "Verwendens" von Daten entspricht dem Begriff "Verarbeiten" in der Richtlinie, in der definitorisch zwischen "Verarbeiten" (im österreichischen Sinn) und "Übermitteln" nicht unterschieden wird. Eine solche Begriffsbildung scheint – schon weil sie im Widerspruch zum Sprachgebrauch steht – nicht optimal, weshalb der österreichischen Tradition folgend weiter die Begriffe "verarbeiten" und "übermitteln" unterschieden werden und dem Überbegriff "verwenden" untergeordnet werden (vgl. auch die Ausführungen zu Z. 12, 13 und 15).

Zu Z. 12, 13 und 15:

Der Begriff des "Verarbeitens" bedeutet, dass das "Ermitteln" in den Verarbeitungsbegriff miteinbezogen wurde; Grund hiefür war eine möglichst weit gehende Angleichung an die Terminologie der Richtlinie. Dass das "Übermitteln" jedoch – so wie bisher – im Verarbeitungsbegriff nicht inkludiert ist und daher vom Sprachgebrauch der Richtlinie abweicht, hat seinen Grund in den unterschiedlichen Zulässigkeitsvoraussetzungen für diese beiden Tätigkeitsarten, weshalb sie auch als getrennte Begriffe aufrechterhalten werden mussten. Dass die Richtlinie dies nicht tut, hat sich bereits als Mangel erwiesen (vgl. etwa die Unklarheiten in Art. 25 und 26 über den dort – undefiniert – gebrauchten Terminus "übermitteln".)

Als "Übermitteln" wird auch die Verwendung von Daten für ein anderes Aufgabengebiet beim selben Auftraggeber verstanden. Ein "Aufgabengebiet" ist eines von mehreren Tätigkeitsfeldern eines Auftraggebers, das in seinem Umfang nach der Verkehrsauffassung geeignet ist, für sich allein den gesamten Geschäftsbereich eines Auftraggebers zu bilden. Das "Aufgabengebiet" wäre also im privaten Bereich z.B. in etwa mit dem Umfang einer Gewerbeberechtigung gleichzusetzen, im öffentlichen Bereich mit einem Kompetenztatbestand (im Sinne der Art. 10 bis 15 B-VG).

Zu Z. 16:

Die Definition der "Zustimmung" gibt weitestgehend den diesbezüglichen Text der Richtlinie (Art. 2 lit. h) wieder. Es ist darauf hinzuweisen, dass eine datenschutzrechtliche Zustimmung nicht unbedingt ausdrücklich und schriftlich vorliegen muss: Die Ausdrücklichkeit ist nur bei der Verwendung sensibler Daten notwendig; die Schriftlichkeit wird nur von Fall zu Fall dann notwendig sein, wenn es darum geht nachzuweisen, dass die Zustimmung zweifelsfrei vorliegt.

4. Zu § 4:

Wie schon die Datenschutzkonvention des Europarates (ETS 108) enthält auch die Richtlinie 95/46/EG in einem Katalog "Grundsätze für die Datenqualität". Dieser Katalog wurde nunmehr ausdrücklich – in sprachlich gekürzter Form – auch in das NÖ Datenschutzgesetz **(§ 4 Abs. 1)** aufgenommen. Für die österreichische Rechtsordnung ist dieser Katalog im Hinblick darauf, dass die Datenschutzkonvention des Europarates Bestandteil der österreichischen Rechtsordnung ist, keine Neuerung.

Eine Verwendung von Daten "nach Treu und Glauben" **(Z. 1)** liegt nur dann vor, wenn der Betroffene über die Umstände des Datengebrauchs und das Bestehen und die Durchsetzbarkeit seiner Rechte nicht irregeführt oder im Unklaren gelassen wird. Wichtig für die Verwirklichung dieses Gebots sind vor allem die Bestimmungen des 4. Abschnitts des vorliegenden Entwurfs über die Publizität der Datenanwendung.

Aus dem Gebot der Verwendung "in rechtmäßiger Weise" ergibt sich u.a. auch, dass der Auftraggeber eine ausreichende rechtliche Befugnis bzw. Zuständigkeit für jene Art der Benützung von Daten, die er mit seiner Datenanwendung bezweckt, besitzen muss.

Das in **Z. 2** statuierte Zweckbeschränkungsprinzip findet im vorliegenden Gesetzentwurf in folgenden Bestimmungen seine Umsetzung:

- Wichtig hiefür ist zunächst die Definition des Übermittlungsbegriffs in § 3 Z. 15: Jeder Zweckwechsel ist eine "Übermittlung"; diese liegt nicht nur dann vor, wenn Daten an einen Dritten weitergegeben werden, sondern auch dann, wenn derselbe Auftraggeber Daten selbst für ein anderes Aufgabengebiet (weiter)verwendet.
- Jede Übermittlung bedarf einer besonderen rechtlichen Grundlage; sind die Voraussetzungen des § 7 Abs. 2 und 3 nicht gegeben, ist eine Übermittlung von Daten unzulässig.

Wenn in Z. 2 statuiert wird, dass eine Weiterverwendung von Daten nur zulässig sein soll, wenn dies mit dem ursprünglichen Ermittlungszweck "nicht unvereinbar" ist, so sei dazu angemerkt, dass diejenigen innerbetrieblichen Datenverwendungen, die der Aufrechterhaltung und Optimierung der Organisation (wie z.B. Rechnungswesen und Controlling) oder der Analyse und Planung dienen, jedenfalls **nicht** als eigener Verwendungszweck zu

sehen sind, der mit dem Zweck der ursprünglichen Datenermittlung (z.B. im Rahmen des Abschlusses eines Handelsgeschäftes) **"unvereinbar"** ist.

Das Gebot der sachlichen Richtigkeit **(Z. 4)** ist so zu verstehen, dass Richtigkeit **im Hinblick auf den deklarierten Zweck der Datenanwendung** gefordert ist: Lautet der deklarierte Zweck etwa "Verzeichnis von Straftätern", dann dürfen Personen, die einer Straftat nur verdächtigt sind, in dieses Verzeichnis nicht aufgenommen werden; anders dann, wenn ein "Verzeichnis der Verdachtsfälle" geführt wird. In diesem Zusammenhang muss jedoch ausdrücklich darauf hingewiesen werden, dass bei Datensammlungen klar erkennbar sein sollte, welches Ausmaß an objektiver Richtigkeit die gespeicherten Daten voraussichtlich besitzen; handelt es sich um sogenannte "weiche" Daten, wird eine regelmäßige Überprüfung auf Aktualität besonders wichtig sein, um ungerechtfertigte Nachteile für Betroffene zu vermeiden.

5. Zu § 5:

Die Richtlinie bezieht sich in Art. 27 auf so genannte "Verhaltensregeln", die nicht-staatliche Institutionen, wie z.B. Berufsverbände, zur näheren Durchführung von einzelstaatlichem Datenschutzrecht für einzelne Branchen und Berufszweige ausarbeiten können. Aus der Sicht der österreichischen Rechtsordnung scheint ein sinnvoller Anwendungsbereich von derartigem "soft law" vor allem bei der näheren Umschreibung dessen zu bestehen, was in einer bestimmten Branche als Datenverwendung nach "Treu und Glauben" anzusehen wäre; weiters wären solche Verhaltensregeln z.B. auch geeignet, um die Rollenverteilung von Auftraggeber und Dienstleister bestimmter Konstellationen ausdrücklich festzuschreiben oder um das Ausmaß der Informationsverpflichtung gegenüber dem Betroffenen bei bestimmten Arten von Datenanwendungen näher festzulegen. Solche Regeln haben freilich keinen verbindlichen Charakter, wären aber bei freiwilliger Befolgung durch die Mehrzahl der Beteiligten sicher ein wertvolles Mittel für die effektive Verwirklichung von Datenschutz in wichtigen Bereichen des täglichen Lebens. Um zu vermeiden, dass durch solche Verhaltensregeln rechtswidrige Handlungsanleitungen aufgestellt werden, bedarf es einer Prüfung, die jedoch nicht von der Datenschutzkommission vorgenommen werden soll, um die Unabhängigkeit der Entscheidungsfindung im einzelnen Beschwerdefall nicht zu präjudizieren. Abs. 2 beruft daher das für Angelegenheiten des Datenschutzes zuständige oberste Organ, die Landesregierung, zu einer Begutachtung der Verhaltensregeln.

6. Zu § 6:

Abs. 1 schreibt Auftraggeberverantwortung für Datenanwendungen ausdrücklich fest. Es ist festzuhalten, dass es sich um die Formulierung eines **Grundsatzes** handelt.

Abs. 2 dient der Umsetzung von Art. 4 Abs. 2 der Richtlinie.

7. Zu § 7:

§ 7 enthält die generelle Regel für die Beurteilung der Zulässigkeit einer konkreten Datenverwendung. Die Zulässigkeit einer konkreten Datenanwendung hat zwei Voraussetzungen:

– die Berechtigung des Auftraggebers und
– die Berücksichtigung der schutzwürdigen Interessen der Betroffenen.

Hinzu treten bei Übermittlungen die in Abs. 2 genannten zusätzlichen Erfordernisse.

Der Grundsatz der Verhältnismäßigkeit ist in Abs. 3 im Hinblick auf – zulässige – Eingriffe in das Grundrecht auf Datenschutz ausdrücklich nochmals festgeschrieben.

8. Zu § 8:

Die Zulässigkeit einer Datenanwendung erfordert gemäß § 7 u.a., dass "schutzwürdige Geheimhaltungsinteressen nicht verletzt werden".

Dieses Erfordernis bedarf näherer Festlegungen, um vollziehbar zu sein. Dies geschieht

– für die **nichtsensiblen Daten** in Form einer Generalklausel (§ 8 Abs. 1) mit einzelnen wichtigen Beispielen (§ 8 Abs. 2 bis 4),
– für **sensible Daten** in Form eines taxativen Katalogs der zulässigen Verwendungsfälle (§ 9).

Durch diese Regelungstechnik wird die von der Richtlinie vorgegebene Kasuistik mit der in österreichischen Gesetzen üblichen Präferenz für generelle Regelungen in Einklang gebracht und überdies die von Art. 8 Richtlinie geforderte Verbotswirkung für die im Art. 8 der Richtlinie nicht erwähnten Fälle der Verwendung sensibler Daten erreicht.

§ 8 Abs. 2 nennt zwei Fälle, in welchen kein Geheimhaltungsanspruch besteht. Zum ersten Fall – der Verwendung zulässigerweise veröffentlichter Daten – ist anzumerken, dass bei allen Datenanwendungen, die solche Daten enthalten, jeweils die Frage zu stellen ist, ob sie **ausschließlich** veröffentlichte Daten enthalten (z.B. bei einem Telefon-Teilnehmerverzeichnis) oder ob nicht auch zusätzliche, durch **Auswertung** der veröffentlichten Daten gewonnene Daten in der Datenanwendung enthalten sind, die ihrerseits nirgends veröffentlicht sind.

Da im Übrigen auch eine andere Form der Aufbereitung veröffentlichter Daten neue – nicht veröffentlichte – Informationen liefern kann, kann nicht ausgeschlossen werden, dass in besonderen Konstellationen schutzwürdige Geheimhaltungsinteressen doch berührt werden, weshalb das Widerspruchsrecht nach § 23 ausdrücklich aufrechterhalten wird.

Um die praktische Anwendung des NÖ Datenschutzgesetzes zu erleichtern, werden in § 8 Abs. 3 einige der wichtigsten Fälle angeführt, in welchen durch die Datenverwendung keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden, weil es sich um zulässige Eingriffe handelt. Dieser Katalog ist in keiner Weise erschöpfend und beschränkt sich im Übrigen auf Falltypen, bei welchen die Verletzung schutzwürdiger Geheimhaltungsinteressen **immer** auszuschließen ist. Nicht aufgenommen in den Katalog wurden daher Verwendungskonstellationen, in welchen die Verletzung schutzwürdiger Geheimhaltungsinteressen zwar unwahrscheinlich ist, aber doch nicht von vornherein ausgeschlossen werden kann, sodass eine Beurteilung von Fall zu Fall notwendig ist (ein Beispiel hiefür wäre die Datenverwendung im Rahmen vorvertraglicher Maßnahmen – vgl. Art. 7 lit. b Richtlinie 95/46/EG).

Ein gesondertes Problem stellt die Verwendung von strafrechtsbezogenen Daten dar. Solche Daten sind nach der Richtlinie nicht "sensible Daten", werden aber – zu Recht – in die Nähe dieser Daten gerückt (vgl. Art. 8 Abs. 5 Richtlinie). Die Verarbeitung strafrechtsbezogener Daten muss daher möglichst beschränkt bleiben, weshalb Abs. 4 Z 3 Grenzen zieht, innerhalb welcher die Verwendung dieser Daten auch durch private Auftraggeber zulässig sein soll.

9. Zu § 9:

Die Zulässigkeit der Verwendung sensibler Daten ist weit gehend durch die Richtlinie 95/46/EG vorgegeben: § 9 gibt zunächst die in Art. 8 Abs. 2 und 3 Richtlinie statuierten Ausnahmen vom Verwendungsverbot wieder. Hinzu treten

- die Ausnahme der Z 2, in der kein Geheimhaltungsanspruch besteht,
- die Ausnahme der Z 10, soweit sie sich auf Verarbeitungen für private Zwecke bezieht, da für diese Datenverwendungen die Richtlinie nicht anzuwenden ist (Art. 3 Abs. 2, 2. Anstrich, Richtlinie),
- die Ausnahmen nach Z 3, Z 4 und Z 5 sowie nach Z 10 hinsichtlich § 16 und § 17: In allen diesen Fällen ergibt sich die Zulässigkeit der Ausnahme vom Verwendungsverbot aus Art. 8 Abs. 4 Richtlinie, da diese Bestimmungen des § 9 die Zulässigkeit der Verwendung von Daten "aus Gründen eines wichtigen öffentlichen Interesses" vorsehen (in Z. 10 z.B. für Zwecke von wissenschaftlicher Forschung und Statistik, woran gemäß Erwägungsgrund 34 der Richtlinie ein wichtiges öffentliches Interesse besteht).

Zum Inhalt der einzelnen Ziffern des § 9 ist Folgendes ergänzend anzumerken:

1. Ein wichtiges öffentliches Interesse im Sinne der Z 3 ist auch in den Interessen der Aufsicht über bestimmte Wirtschaftszweige zu erblicken: Gesetze, die die Verwendung von Daten für Zwecke einer besonderen Wirtschaftsaufsicht vorsehen, erfüllen ein wichtiges öffentliches Interesse; dies trifft etwa zu bei gesetzlichen Datenverwendungsbestimmungen im Rahmen der Banken- oder Versicherungsaufsicht.

2. Die Verwendung sensibler Daten zur Rechtsverteidigung gemäß Z 9 schließt naturgemäß die Zulässigkeit der Verwendung dieser Daten im Vorfeld einer gerichtlichen – oder verwaltungsbehördlichen – Auseinandersetzung ein, also z.B. auch die Verwendung im Rahmen des Versuchs einer außergerichtlichen Streitbeilegung.

10. Zu § 10:

Die Verantwortung des Auftraggebers hinsichtlich einer Kontrolle des Dienstleisters wird durch jene Rechtsvorschriften oder Standesregeln beschränkt, die eine Einflussnahme des Auftraggebers auf die Auftragsdurchführung durch den Dienstleister ausschließen. In welchen Fällen aus der Pflicht zur selbständigen Aufgabenerfüllung durch den Auftragnehmer gemäß § 3 Z. 5 sogar die datenschutzrechtliche Auftraggebereigenschaft abzuleiten ist, wird in Form von Verhaltensregeln im Sinne des § 5 ausdrücklich darzustellen sein.

Die Anzeigepflicht an die Datenschutzkommission ist daher auf die Heranziehung von (privaten) Dienstleistern bei Datenanwendungen, die infolge ihrer Sensibilität der Vorabkontrolle unterliegen, beschränkt.

11. Zu § 11:

Diese Bestimmung entspricht dem DSG 2000.

12.Zu §§ 12 und 13:

Als Ergebnis der durch die Richtlinie angestrebten Harmonisierung der datenschutzrechtlichen Rechtsvorschriften der EU-Mitgliedstaaten soll die datenschutzrechtliche Kontrolle des Datenverkehrs zwischen EU-Staaten entfallen (**§ 10 Abs. 1** erster Satz). Dieses Prinzip gilt allerdings **nicht** hinsichtlich der Datenverwendung für Zwecke der so genannten "dritten Säule" (Zusammenarbeit der EU-Mitgliedstaaten im Bereich Justiz und Inneres), weil diese Bereiche von der Richtlinie nicht erfasst sind und daher nicht dem Harmonisierungsgebot unterliegen, was Voraussetzung für den unbeschränkten Datenverkehr wäre.

Über die im ersten Satz des Abs. 1 erwähnten Fälle hinaus sind auch die in **Abs. 3 und 4** geregelten Fälle des **Datenverkehrs ins Ausland ohne Beschränkungen zulässig;** dies entspricht den Bestimmungen des Art. 26 Abs. 1 der Richtlinie.

Für alle anderen Fälle des Datenverkehrs mit dem Ausland gilt der Grundsatz, dass der Datenexport nur zulässig ist,

– wenn beim Empfänger ein **"angemessenes Datenschutzniveau"** besteht (Art. 25 Abs. 1 Richtlinie 95/46/EG) oder

– wenn der Auftraggeber der Übermittlung (Überlassung) gegenüber der Datenschutzkommission das Vorliegen **ausreichender Garantien** für den Schutz der Betroffenenrechte im Ausland glaubhaft macht (Art. 26 Abs. 2 Richtlinie 95/46/EG).

Für die Frage, wie festgestellt wird, ob ein "angemessenes Datenschutzniveau besteht", bietet der vorliegende Entwurf zwei alternative Antworten:

Wenn ein Staat generell ein angemessenes Datenschutzniveau besitzt, kann er in die Verordnung der Landesregierung gemäß § 12 Abs. 2 aufgenommen werden, was bewirkt, dass der Datenverkehr mit diesem Staat zur Gänze ohne Beschränkungen zulässig ist. (Eine solche generelle Aussage ist auch hinsichtlich der Verwirklichung von Datenschutz in EU-Mitgliedstaaten betreffend die so genannte "dritte Säule" zulässig). In allen anderen Fällen muss die Beurteilung von Fall zu Fall geschehen, und zwar anlässlich des Genehmigungsverfahrens gemäß § 13 Abs. 2 Z 1.

Die zum Zweck einer einheitlichen Beurteilung dieser Fragen in allen EU-Mitgliedstaaten vorgesehenen Mitteilungs- und Durchführungspflichten sind in § 31 umgesetzt.

13. Zu § 14:
Diese Bestimmung entspricht sinngemäß dem DSG 2000.

14. Zu § 15:
Die Verpflichtung des Auftraggebers und des Dienstleisters – einschließlich ihrer Mitarbeiter – zur Geheimhaltung von **Daten, die** ihnen **auf Grund** ihrer **berufsmäßigen Beschäftigung bekannt** geworden sind, ist bereits im geltenden DSG des Bundes enthalten.

§ 15 gilt sowohl für Auftraggeber (und Dienstleister) des privaten Bereichs als auch für Auftraggeber (und Dienstleister) des öffentlichen Bereichs sowie für deren Mitarbeiter. Diese Bestimmung verweist auf § 15 DSG 2000.

15. Zu § 16:
Die Richtlinie 95/46/EG spricht an mehreren Stellen deutlich aus, dass eine besondere, privilegierende Stellung von wissenschaftlicher Forschung und Statistik bei der Verwendung personenbezogener Daten als sachlich gerechtfertigt angesehen wird. Dementsprechend enthält der vorliegende Entwurf eine eingehende datenschutzrechtliche Regelungen für diesen Bereich der Verwendung personenbezogener Daten.

Was die Begriffe "wissenschaftliche Forschung" und "Statistik" betrifft, geht die vorliegende Regelung in Beachtung der Terminologie der Richtlinie 95/46/EG von folgendem Begriffsverständnis aus:

"Wissenschaftliche Forschung" soll nicht einen inhaltlich abgegrenzten Bereich bezeichnen – etwa in der Richtung, dass nur Grundlagenforschung erfasst und angewandte Forschung ausgeschlossen wäre –, sondern als Bereich verstanden werden, in dem eine bestimmte Methode der Vorgangsweise, nämlich eine "wissenschaftliche", angewendet wird. Dass hiefür nicht der Ausdruck "Forschung" allein verwendet wird, ist in der Terminologie der Richtlinie begründet: Eine abweichende Begriffsbildung könnte zu Interpretationsschwierigkeiten führen.

Auch der Begriff **"Statistik"** wird dahingehend verstanden, dass es sich um methodologisch **"wissenschaftliche** Statistik" handelt, da nur unter dieser Voraussetzung eine Privilegierung sachlich zu rechtfertigen ist. Abgesehen davon soll aber dieser Begriff sowohl die so genannte "amtliche Statistik" als auch sonstige (mit wissenschaftlichen Methoden durchgeführte) Statistik umfassen.

16. Zu § 17:

Gemäß Art. 21 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 sehen die Mitgliedstaaten vor, dass für Verarbeitungen, die von der Meldung ausgenommen sind, der für die Verarbeitung Verantwortliche oder eine andere von den Mitgliedstaaten benannte Stelle zumindest die in Art. 19 Abs. 1 Buchstaben a) bis e) vorgesehenen Angaben auf Antrag jedermann in geeigneter Weise verfügbar macht. Dies wird mit dieser Bestimmung vorgesehen.

17. Zu § 18:

Bei Verarbeitungen, die "spezifische Risiken für die Rechte und Freiheiten von Personen beinhalten können", sieht die Richtlinie 95/46/EG vor, dass sie einer so genannten **"Vorabkontrolle"** zu unterwerfen sind, d.h. dass sie vor ihrer Aufnahme durch die unabhängige Kontrollinstanz auf ihre Zulässigkeit zu prüfen sind. Dementsprechend ist in **Abs. 1** festgelegt, welche Kategorien von Datenanwendungen erst nach Prüfung und Registrierung aufgenommen werden dürfen. Diese Kategorien wurden unter Berücksichtigung der in der Richtlinie in Art. 18 Abs. 2 erster Anstrich der Richtlinie 95/46/EG erwähnten Beurteilungskriterien für das Gefährdungspotential von Datenverarbeitungen bestimmt.

Strafrechtsbezogene Daten (Z. 2) werden von der Richtlinie zwar nicht als sensible Daten bezeichnet, aber hinsichtlich der Schutzwürdigkeit als "sensibilitätsnah" behandelt (vgl. Art. 8 Abs. 5 Richtlinie), weshalb ihre Unterstellung unter die Vorabkontrolle sachlich geboten erscheint.

Der Vorabkontrolle sind weiters Datenanwendungen unterworfen, die die **Auskunftserteilung über die Kreditwürdigkeit** von natürlichen Personen zum Gegenstand haben **(Z. 3)**. Unter "Auskunftserteilung" ist nicht die aus den Unterlagen des Rechnungswesens in einem Unternehmen hervorgehende Information über kreditrelevantes Verhalten der eigenen Kunden (potentiellen Kunden) zu verstehen; von Z. 3 erfasst sollen vielmehr nur jene Datenanwendungen sein, deren ausschließlicher Zweck die Auskunftserteilung ist und zwar an Außenstehende für deren Zwecke (Vereinsmitglieder wären in diesem Sinn als Außenstehende zu betrachten, wenn etwa ein Verein ein Kreditauskunftssystem betreibt).

18. Zu § 19:
Hinsichtlich des Inhalts von Meldung, wonach in Erfüllung der Erfordernisse der Richtlinie 95/46/EG allgemeine Angaben über die im konkreten Fall bestehenden Daten Sicherheitsmaßnahmen zu machen sind, wird auf Abs. 1 Z. 6 verwiesen.

Hinsichtlich des Verfahrens der Vorabkontrolle ist ausdrücklich vorgesehen, dass bei Untätigkeit der Datenschutzkommission die Verarbeitung von Daten jedenfalls zwei Monate nach Abgabe der Mitteilung aufgenommen werden kann. Wenn hingegen im Fall eines Verbesserungsauftrages im Vorabkontrollverfahren entschieden wird, dass die Verarbeitung noch nicht aufgenommen werden darf, gelten die Entscheidungsfristen des AVG einschließlich der Möglichkeit der Säumnisbeschwerde für die Entscheidung darüber, ob die aufgetragenen Verbesserungen vorgenommen wurden und davon abgeleitet, ob die Verarbeitung aufgenommen werden darf. Diese Bestimmung wurde den Bestimmungen der §§ 19 und 20 DSG 2000 nachgebildet.

19. Zu § 20:
Diese Bestimmung setzt Art. 12 der Richtlinie 95/46/EG um.

§ 20 Abs. 3 regelt, in welchen Fällen im öffentlichen Interesse oder im Interesse Dritter keine Auskunft zu geben ist. Die Zulässigkeit dieser Ausnahmen stützt sich auf Art. 13 der Richtlinie 95/46/EG. Im Übrigen wird – in Übereinstimmung mit Art. 13 der Richtlinie – auch der Fall einbezogen, dass das Auskunftsrecht zum Schutz des Betroffenen einzuschränken ist; dies wird freilich nur in wenigen Ausnahmefällen gerechtfertigt sein (z.B. im medizinischen Bereich oder hinsichtlich von Auskünften aus dem Strafregister).

20. Zu § 21:
In dem Bestreben, einen Interessensausgleich zwischen dem Betroffenen und dem Auftraggeber zu erzielen, statuiert daher Abs. 1, dass der Betroffene in dem ihm zumutbaren Ausmaß mitwirken muss. Abs. 3 regelt, dass die Auskunft dann unentgeltlich zu erteilen

ist, wenn die Auffindung der zu beauskunftenden Daten für den Auftraggeber keine besondere Belastung darstellt. In allen anderen Fällen ist die Auskunft kostenpflichtig, wobei ein niedriger Grundtarif im Gesetz festgelegt ist, von dem bei tatsächlich erwachsenden höheren Kosten abgewichen werden darf. Auch Portokosten sind den tatsächlich erwachsenden Kosten zuzuzählen. Ob derartige Abweichungen gerechtfertigt sind, wäre in einem Verfahren vor der Datenschutzkommission gemäß § 26 Abs. 1 überprüfbar.

21. Zu § 22:

§ 22 stellt die zusammenfassende Regelung des Rechtes auf Richtigstellung oder Löschung dar. Es wurde hiebei eine Vereinheitlichung des Verfahrens und eine Vereinfachung der Regelungen angestrebt. Im § 22 Abs. 1 wird zunächst klar gestellt, dass die Verpflichtung zur Richtigstellung oder Löschung von Daten den Auftraggeber auch dann trifft, wenn der Betroffene dies nicht eigens beantragt hat. Weiters werden Klarstellungen gegeben, wann Unvollständigkeit und wann Unzulässigkeit der Verarbeitung in bestimmten Konstellationen vorliegt. Abs. 6 trägt dem Umstand Rechnung, dass manche Datenanwendung nach ihrem besonderem Zweck eine Löschung von Daten in der Form, dass Daten nicht mehr sichtbar sind, nicht gestatten. Dies wird überall dort der Fall sein, wo die lückenlose Dokumentation eines Geschehens Gegenstand der Datenverarbeitung ist (zB bei der Führung von Krankengeschichten).

22. Zu § 23:

Ein eigenes Widerspruchsrecht hat sich bisher im österreichischen Datenschutzrecht nicht gefunden. Die Richtlinie 95/46/EG sieht ein solches in Art. 14 vor.
Ausgehend von der zum Teil sehr allgemeinen Formulierung der Zulässigkeitsvoraussetzung für Datenverarbeitungen in Art. 7 der Richtlinie (insbesondere lit. e und f) enthält die Richtlinie als Korrekturmöglichkeit ein Widerspruchsrecht, wonach der Betroffene verlangen kann, dass er aus "sich aus seiner besonderen Situation ergebenden Gründen" aus einer Datenanwendung, gegenüber der das Widerspruchsrecht geltend macht, gelöscht wird.
Zur Frage, wo der Unterschied zwischen einer Beschwerde (Klage) wegen unzulässiger Verarbeitung von Daten nach den §§ 26 oder 27 und der Ausübung des Widerspruchrechts nach § 28 Abs. 1 liegt, ist Folgendes auszuführen:
Die Richtlinie enthält in Art. 14 keine klare Aussage über diese Frage und gibt auch keinen Hinweis auf möglicherweise unterschiedliche Folgen. Daraus, dass in Art. 14 aber auch auf das Widerspruchsrecht im Bereich der Verwendung von Daten für Marketingzwecke Bezug genommen wird, könnte folgender Schluss gezogen werden:
Die Ausübung des Widerspruchsrechts hat keinen Einfluss auf die rechtliche Zulässigkeit der Datenanwendung an sich. Sie bewirkt nur eine individuell auf den (erfolgreich) Widersprechenden begrenzte Löschungspflicht, bedeutet aber nicht, dass die gesamte Datenanwendung wegen Rechtswidrigkeit einzustellen wäre. Die erfolgreiche Ausübung des

Widerspruchsrechts wird daher – zumindest grundsätzlich – auch keinen Schadenersatzanspruch begründen können.

In Abs. 3 wird eine zusätzliche Spielart des Widerspruchsrechts ausdrücklich geregelt, die in der Praxis nach den bisherigen Erfahrungen bedeutsam ist und nur die Nutzanwendung des bereits zu Abs. 1 Gesagten auf eine besondere Konstellation darstellt: Es gibt wiederholt Anwendungsfälle, in welchen bei einer Durchschnittsbetrachtung eine Verletzung schutzwürdiger Geheimhaltungsinteressen infolge des Zwecks der Datenverarbeitung und der verwendeten Datenarten unwahrscheinlich ist (Beispielsfälle wären etwa Verzeichnisse österreichischer Gewerbetreibender, die für Exportförderungszwecke verwendet werden; Einwohnerverzeichnisse; Verzeichnisse von Fernsprechteilnehmern, Telefaxanschlüssen, E-Mail-Adressen, usw.). Derartige öffentlich zugängliche Verzeichnisse beruhen zum größten Teil nicht auf ausdrücklichen gesetzlichen Regelungen. Um einen fairen Interessensausgleich zu gewährleisten, scheint es sinnvoll, Personen ein Widerspruchsrecht gegen die Aufnahme in solche Verzeichnisse einzuräumen, wenn sie in Abweichung von der durchschnittlichen Einschätzung der Geheimhaltungsinteressen eine Verletzung ihrer Interessen durch Aufnahme ihrer Daten in ein solches Verzeichnis befürchten. Durch die Möglichkeit des Widerspruchs wäre gewährleistet, dass einerseits Verzeichnisse dieser Art, die von der großen Mehrheit der Bevölkerung als sinnvoll und nützlich empfunden werden, legalerweise existieren können und andererseits Interessenslagen, die vom Durchschnitt abweichen, entsprechend berücksichtigt werden können und diese Berücksichtigung auch einfach durchzusetzen ist.

23. Zu § 24:

Diese Regelung bezieht sich auf indirekt personenbezogene Daten.

24. Zu § 25:

Die Richtlinie 95/46/EG misst der Kontrolle von Datenanwendungen außerhalb förmlicher Beschwerdeverfahren große Bedeutung zu. Diese Kontrolle muss gemäß der Richtlinie auch im privaten Bereich möglich sein. Sie ist von einer unabhängigen Kontrollstelle wahrzunehmen und hat das Recht der Kontrollstelle zu beinhalten, Einschau in Datenverarbeitungen und Unterlagen zu nehmen, Auskünfte zu verlangen und dem Auftraggeber Empfehlungen und Ermahnungen zu erteilen; sie kann bis zu einem gewissen Grad auch rechtsförmliche Akte umfassen, soweit zB eine Kompetenz zur vorläufigen Untersagung der Weiterführung von Datenverarbeitungen besteht.

Das in Österreich traditionelle System des Vollzugs von Datenschutz hat bisher den Schwerpunkt auf rechtsförmliche Entscheidung durch die Datenschutzkommission bzw. durch die Gerichte gelegt und nur im öffentlichen Bereich eine Kontrolle laufender Datenverarbeitungen vorgesehen. Im vorliegenden Entwurf sind nun die Kontrollbefugnisse in der Weise umgesetzt, dass die Datenschutzkommission als unabhängige Kontrollstelle den öffentlichen und den privaten Bereich zu kontrollieren hat, und zwar entweder aus

Anlass eines Anbringens eines Bürgers oder auch in Fällen, die ein erhöhtes Gefährdungspotential besitzen, ohne einen solchen Anlass. Rechtsförmliche Entscheidungen über behauptete Datenschutzverletzungen werden hingegen so wie bisher von der Datenschutzkommission zu erlassen sein, wenn sie Auftraggeber des öffentlichen Bereichs betreffen, und von den ordentlichen Gerichten, wenn sie Auftraggeber des privaten Bereichs betreffen.

Die Verpflichtung zur möglichsten Schonung der Rechte des Auftraggebers (Dienstleisters) bedeutet auch, dass eine Einschau grundsätzlich nur innerhalb der Betriebszeiten vorgenommen werden darf.

Die Einschau durch die DSK dient einem eng begrenzten Ziel, nämlich der Durchsetzung von Datenschutz. Es erscheint daher sachlich gerechtfertigt, die Verwertung der durch die Einschau gewonnenen Informationen auf datenschutzrechtliche Belange zu begrenzen; die insbesondere in § 26 StPO und § 158 BAO statuierte Pflicht zur Offenlegung von Informationen und die Verpflichtung zur Erstattung von Anzeigen nach § 84 StPO und § 81 FinStrG wurde daher – soweit keine datenschutzrechtlich relevanten Straftatbestände betroffen sind – auf besonderes schwer wiegende (gerichtlich ahndbare) Straftaten beschränkt, nämlich auf Verbrechen mit einer Mindeststrafdrohung von fünf Jahren. Hiedurch wird auch gewährleistet, dass die im Bankwesengesetz (§ 41 Abs. 6) und im Wertpapieraufsichtsgesetz (§ 30 Abs. 3) im Interesse der Wahrung des Bankgeheimnisses enthaltenen Regelungen nicht unterlaufen werden.

25. Zu § 26:

Die Datenschutzkommission übt neben ihrer Kontrollfunktion auch eine quasi-richterliche Entscheidungsfunktion in ihrer Rolle als Behörde gemäß Art. 133 Z 4 B-VG aus. Sie erkennt in rechtsförmlichen Verfahren mit Bescheid über Beschwerden wegen behaupteter Verletzungen des Datenschutzgesetzes durch einen Auftraggeber des öffentlichen Bereichs. Eine Besonderheit des Entwurfes ist die nunmehrige umfassende Zuständigkeit für Verletzungen des Auskunftsrechtes (Abs. 1), gleichgültig, ob diese einem Auftraggeber des öffentlichen Bereichs oder einem Auftraggeber des privaten Bereichs zur Last gelegt werden. Hinsichtlich aller anderen behaupteten Verletzungen ist die Datenschutzkommission nur dann zuständig, wenn sie einen Auftraggeber des öffentlichen Bereichs betreffen (Abs. 2), insgesamt aber immer nur im Hinblick auf die Prüfung von Handlungen, die weder der Gerichtsbarkeit noch der Gesetzgebung zuzurechnen sind, wobei die Zurechnung nach funktionalen Gesichtspunkten vorzunehmen ist.

26. Zu § 27:

Der Betroffene hat Anspruch auf Unterlassung und Beseitigung eines dem NÖ Datenschutzgesetz widerstreitenden Zustands. Ist Verursacher ein Auftraggeber des privaten Bereichs, so sind diese Ansprüche vor den ordentlichen Gerichten durchzusetzen. Einzige

Ausnahme hievon ist die Durchsetzung des Auskunftsrechts, für die in Hinkunft immer die Datenschutzkommission zuständig sein soll.

Gegenüber den bisherigen Bestimmungen über das zivilgerichtliche Verfahren in Datenschutzsachen bringt die vorliegende Regelung insofern eine Neuerung, als die Datenschutzkommission an Stelle des Betroffenen bei dem zuständigen ordentlichen Gericht Klage zur Feststellung der Rechtmäßigkeit einer Datenverwendung erheben kann. Diese Möglichkeit ist auf vermutete schwer wiegende Datenschutzverletzungen beschränkt und soll für solche Fälle, an deren Klärung somit auch ein öffentliches Interesse besteht, das Prozessrisiko des Betroffenen vermeiden. Auf der Grundlage des gerichtlichen Feststellungsurteils kann der Betroffene sodann entscheiden, ob er seine Unterlassungs- und Schadenersatzansprüche selbst weiter verfolgen will.

Die Möglichkeit einer Nebenintervention gemäß § 17ff ZPO wurde hingegen beibehalten. Auch die Eintragung von gerichtlichen Urteilen in das Datenverarbeitungsregister hat sich als praktisch nicht bedeutsam erwiesen, weshalb dies nicht mehr ausdrücklich in den Gesetzesentwurf aufgenommen wurde. Für die Veröffentlichung von richtungsweisenden gerichtlichen Entscheidungen scheinen die üblichen Publikationswege ausreichend.

27. Zu § 28:

Diese Bestimmung stellt lediglich einen Hinweis auf die im Zivilrecht vorhandenen Schadenersatzregelungen dar. Im Übrigen werden die für den Bereich des DSG 2000 schadenersatzrechtliche Regelungen übernommen.

28. Zu § 29:

Die Anwendungserfahrung, insbesondere vor der Datenschutzkommission, hat ergeben, dass die Statuierung von Verjährungsfristen (Abs. 1) für die Geltendmachung der Interessen der Betroffenen nach diesem Gesetz sachlich geboten ist: Die Ermittlung von Sachverhalten, die lange zurückliegen, stößt erfahrungsgemäß auf erhebliche Schwierigkeiten und verhindert eine verlässliche Beurteilung des Vorliegens von Datenschutzverletzungen. Auch im eigenen Interesse sollten die Betroffenen daher dazu angehalten werden, behauptete Datenschutzverletzungen möglichst frühzeitig bei der Datenschutzkommission oder bei Gericht anhängig zu machen.

§ 29 Abs. 2 weist ausdrücklich darauf hin, dass auch die Verletzung ausländischen Datenschutzrechtes vor den in Österreich zuständigen Stellen anhängig gemacht werden kann, und zwar insbesondere auch im Rahmen der Kontrolltätigkeit der Datenschutzkommission nach § 25 des Entwurfs.

Durch die Statuierung der Verpflichtung zur Amtshilfe an ausländische Kontrollstellen **(Abs. 4)** – eine Verpflichtung, die in den Rechtsordnungen aller EU-Mitgliedstaaten vorzusehen ist – sollen die Vollziehungsprobleme, die sich aus der Anwendung ausländischen Rechts ergeben, verringert werden.

29. Zu § 30:

Die Richtlinie verlangt von der nationalen Rechtsordnung, dass sie entsprechende Sanktionen für die Ahndung von Verstößen vorsieht (Art. 24 Richtlinie). Im Hinblick auf das Verletzungspotential der Straftatbestände wurde eine Abstufung des Strafrahmens eingeführt:

- Abs. 1 enthält Tatbestände, in welchen eine Verletzung von Rechten tatsächlich stattgefunden hat;
- Abs. 2 zählt Tatbestände auf, in welchen zwar noch keine Verletzung von Rechten des Betroffenen manifest ist, aber Unterlassungen begangen wurden, die eine Gefährdung der Rechte des Betroffenen oder zumindest eine Gefährdung der Durchsetzbarkeit dieser Rechte zur Folge hat.

Die Zurechnung der Verantwortlichkeit für Tathandlungen zu den einzelnen Organen (Mitarbeitern) eines Auftraggebers oder Dienstleisters ist durch § 9 VStG geregelt. Für Auftraggeber des öffentlichen Bereichs bedeutet dies, dass auch interne Organisationsvorschriften zur Beurteilung dieser Frage heranzuziehen sein werden.

Eine wesentliche Änderung gegenüber der bisherigen Rechtslage ist der Umstand, dass die Datenschutzkommission nicht mehr als Berufungsinstanz in Verwaltungsstrafverfahren zuständig ist. Dies deshalb, weil der Grundsatz des fairen Verfahrens es verbietet, dass die Datenschutzkommission einerseits Kontrollrechte ausübt (– und zwar in weit größerem Umfang als dies nach der bisherigen Rechtslage der Fall war –) und im Rahmen dieser Kontrollbefugnisse allenfalls auch Anzeige an die zuständige Strafbehörde erster Instanz erstattet und andererseits als Berufungsinstanz zur Entscheidung über diese Anzeige berufen wäre (vgl. im Übrigen auch das Urteil des EGMR im Fall Bönisch gg. Ö., EuGRZ 1986/127).

30. Zu § 31:

Die Bestimmungen des § 31 ist in unmittelbarer Umsetzung der Richtlinie 95/46/EG notwendig. Sie dient einer gleichmäßigen Entscheidungspraxis in den Fällen des Datenverkehrs mit Drittstaaten durch die Behörden aller EU-Mitgliedstaaten.

31. Zu § 32:

Abs. 1 dient der Umsetzung des Art. 28 Abs. 2 der Richtlinie 95/46/EG.

Abs. 2 dient der gegenseitigen Information zwischen Landesregierung und Datenschutzkommission.

32. Zu § 33:

Diese Bestimmung dient der Angleichung an die Bestimmung des § 56 DSG 2000.

33. Zu § 34:
Mit dem Umsetzungshinweis wird klar gestellt, welche Richtlinie durch dieses Gesetz umgesetzt wird.

34. Zu § 36:
Die Übergangsbestimmung orientiert sich an Art. 32 der Richtlinie 95/46/EG.

Lit. a stellt so wie die Richtlinie 95/46/EG auf den Zeitpunkt der **Annahme** der Richtlinie ab. Für die Ausnahme wurden die zwölf Jahre entsprechend der Richtlinie angenommen.

Lit. b knüpft an die Bestimmung des Art. 32 Z. 2 an, der vorsieht, dass für Verarbeitungen, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschrift bereits begonnen wurden, binnen 3 Jahren mit diesem Gesetz in Einklang zu bringen sind.

Die NÖ Landesregierung beehrt sich daher, den Antrag zu stellen:

Der Hohe Landtag wolle die beiliegende Vorlage der NÖ Landesregierung über den Entwurf eines NÖ Datenschutzgesetzes (NÖ DSG) der verfassungsmäßigen Behandlung unterziehen und einen entsprechenden Gesetzesbeschluss fassen.

NÖ Landesregierung
Dr. P r ö l l
Landeshauptmann

Für die Richtigkeit
der Ausfertigung