BUNDESKANZLERAMT VERFASSUNGSDIENST
GZ ● BKA-810.016/0001-V/3/2007
ABTEILUNGSMAIL ● V@BKA.GV.AT
BEARBEITER ● MAG. ALEXANDER FLENDROVSKY
PERS. E-MAIL ● ALEXANDER.FLENDROVSKY@BKA.GV.AT
TELEFON ● 01/53115/2836

An
alle Bundesministerien sowie
die Sektionen I bis IV, VI und VII des Bundeskanzleramtes
sowie zur Kenntnis an
die Parlamentsdirektion,
alle Ämter der Landesregierungen,
die Verbindungsstelle der Bundesländer beim Amt der NÖ Landesregierung und
alle juristischen Mitarbeiter des Verfassungsdienstes

Antwort bitte unter Anführung der GZ an die Abteilungsmail

Betrifft: Rundschreiben zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz

Das Bundeskanzleramt-Verfassungsdienst hält es für zweckmäßig, seine Empfehlungen zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz gemäß § 1 Abs. 2 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999, zuletzt geändert durch BGBl I Nr. 13/2005[1], zusammenzufassen und zu ergänzen. Es wird ersucht, die gegenständliche Empfehlung bei der Ausarbeitung zukünftiger Gesetzesvorhaben zu beachten.

## 1. Unmittelbare Drittwirkung des Grundrechts auf Datenschutz

Zunächst ist daran zu erinnern, dass das Grundrecht auf Datenschutz sich insoweit von anderen verfassungsmäßig gewährleisteten Rechten unterscheidet, als es jedermann sowohl gegenüber dem Staat als auch gegenüber Privaten zukommt.

## 2. Verfassungsunmittelbare Eingriffsermächtigungen gemäß § 1 Abs. 2 (lebenswichtiges Interesse und Zustimmung des Betroffenen)

1 Paragraphenbezeichnungen in diesem Rundschreiben beziehen sich auf das DSG 2000 in dieser Fassung, sofern nicht ausdrücklich auf eine andere Rechtsvorschrift Bezug genommen wird.

2.1. § 1 Abs. 2 erlaubt Eingriffe in das Recht auf Geheimhaltung zunächst dann, wenn sie im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgen. Für derartige Eingriffe besteht kein Gesetzesvorbehalt, dh sie können unmittelbar auf Grundlage des § 1 Abs. 2 stattfinden, wenngleich sie einfachgesetzlich ausgestaltet bzw. präzisiert werden können, um etwa in einem Rechtsgebiet typischerweise auftretende Fallkonstellationen zu erfassen. Die Richtlinie 95/46/EG über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie – DS-RL) ermöglicht zwar, dass das Verbot der Verwendung sensibler Daten in speziellen gesetzlich geregelten Fällen auch durch die Zustimmung nicht aufgehoben werden darf (also einen Ausschluss der Zustimmung als Eingriffsermächtigung), jedoch sollte dies nur in begründeten Fällen erfolgen (vgl. dazu etwa § 67 des Gentechnikgesetzes, der die Verwendung von Daten aus genetischen Analysen für bestimmte Zwecke ausschließt). Im Bereich der nicht-sensiblen Daten scheint ein genereller Ausschluss der Möglichkeit zur Zustimmung auf einfachgesetzlicher Ebene nicht zulässig.

2.2. Der Begriff des lebenswichtigen Interesses ist eng auszulegen: Ein solches kann etwa im Falle notfallmedizinisch indizierter Eingriffe als gegeben erachtet werden.

2.3. Die Möglichkeit, einen Eingriff in das Recht auf Geheimhaltung (§ 1 Abs. 1) auf die Zustimmung des Betroffenen zu stützen, ist insofern beschränkt, als hier insbesondere auf das – bereits in der DS-RL vorgesehene – Zwangsverbot (vgl. § 4 Z 14) bei Zustimmungserklärungen Rücksicht zu nehmen ist.

2.4. Daher können Regelungen, die eine Pflicht zur Zustimmung vorsehen (ungeachtet ihres Wortlautes und der allfälligen Verwendung des Begriffs „Zustimmung“), nicht auf die Eingriffsermächtigung „Zustimmung“ gestützt werden, da es ihnen an einer wesentlichen Voraussetzung, nämlich der Zwangsfreiheit mangelt. Die Zwangsfreiheit ergibt sich nicht nur aus der einfachgesetzlichen Legaldefinition der Zustimmung (§ 4 Z 14), sondern kann mittelbar bereits aus der unterschiedlichen Struktur der Eingriffsermächtigungen des § 1 Abs. 2 abgeleitet werden: Während die beiden ersten Eingriffsermächtigungen („lebenswichtiges Interesse“ und „Zustimmung“) die individuelle, höchstpersönliche Sphäre des Betroffenen berühren, regelt die dritte Eingriffsermächtigung („überwiegende berechtigte

Interessen anderer“) Fälle, in denen die Notwendigkeit zur Verwendung der Daten außerhalb der Person des Betroffenen liegt.

2.5. Im Bereich der Hoheitsverwaltung kann im Hinblick auf das dieser inhärente Verhältnis von Über- und Unterordnung („imperium“) im Zweifel nicht von der Freiwilligkeit (und damit Wirksamkeit) einer Zustimmung ausgegangen werden. Ist jedoch die Freiwilligkeit unzweifelhaft gegeben, so ist auch hier eine Zustimmung möglich (z. B. zur Weiterleitung von bei einer Behörde befindlichen Unterlagen an einen Dritten als Alternative zu der Möglichkeit, dass der Betroffene diese selbst aushebt und vorlegt).

2.6. Schon das DSG 2000 enthält in seinem einfachgesetzlichen Teil nähere Regelungen zur Zustimmung. Nach § 8 Abs. 1 Z 2 führt die Zustimmung zur Verwendung nicht-sensibler Daten dazu, dass schutzwürdige Geheimhaltungsinteressen nach § 1 Abs. 1 nicht verletzt sind. Auch der Verwendung sensibler Daten kann nach § 9 Z 6 zugestimmt werden. Allerdings muss eine derartige Zustimmung ausdrücklich erfolgen. Nach beiden Bestimmungen sind Zustimmungen jederzeit widerrufbar. Ein Widerruf führt zur Unzulässigkeit der weiteren Datenverwendung. Die Möglichkeit des jederzeitigen Widerrufs wird – ähnlich wie das Zwangsverbot (2.3) - auch dem verfassungsrechtlichen Zustimmungsbegriff des § 1 Abs. 2 zu unterstellen sein und ist daher verfassungsrechtlich geboten.

2.7. Die Zustimmung sollte in besonderen Bestimmungen nur dann vorgesehen werden, wenn vom DSG 2000 abweichende Bestimmungen (s. soeben 2.6.) getroffen werden.

## 3. Eingriffe auf Grund „überwiegender berechtigter Interessen“

3.1. Im Hinblick auf den soeben dargestellten begrenzten Anwendungsbereich der verfassungsunmittelbaren Eingriffsermächtigungen wird in vielen Fällen, in denen Eingriffe notwendig erscheinen, versucht werden müssen, diese auf das Vorliegen überwiegender berechtigter Interessen zurückzuführen. Hinsichtlich der vorzunehmenden **Interessenabwägung** können im Hinblick auf die Vielzahl an vorstellbaren Fallkonstellationen keine allgemein gültigen Aussagen getroffen werden. Dennoch sei beispielhaft auf folgende Entscheidungen hingewiesen:

- In VfSlg. 12.880/1991 hat der Verfassungsgerichtshof die Auslegung der Abgabenbehörden bestätigt, wonach sich Ziviltechniker im Finanzverfahren

nicht auf ihre gesetzliche Verschwiegenheitspflicht berufen dürfen und somit die Interessenabwägung zu Gunsten der Auskunftserteilung vorgenommen.

- Der Rechnungshof hat bei seiner Berichterstattung regelmäßig eine Interessenabwägung zwischen privaten Geheimhaltungsinteressen und dem öffentlichen Interesse der Bekanntgabe der Kontrollergebnisse vorzunehmen. Eine Angabe von Bezügen einzelner Personen unter deren Namensnennung im Tätigkeitsbericht des Rechnungshofes an den Nationalrat ist durch Art. 8 EMRK und auch durch § 1 DSG jedenfalls ausgeschlossen (VfSlg. 17.065/2003 ua.).
- Angesichts der verfassungsrechtlichen Unbedenklichkeit der Anbindung des Beitragsrechts der gewerblichen Sozialversicherung an die im Einkommensteuerbescheid manifestierten steuerpflichtigen Einkünfte ist eine Regelung, welche die Versicherten zur Bekanntgabe dieser Daten verpflichtet, erforderlich und verhältnismäßig. Es ist unvermeidbar, dass mit der Vorlage des Einkommensteuerbescheides der Sozialversicherung auch andere, im Einkommensteuerbescheid enthaltene Daten des Versicherten zur Kenntnis gelangen, welche sie für die Feststellung von Beitragsgrundlagen nicht benötigt. Ebenso unbedenklich ist eine direkte elektronische Datenübermittlung zwischen der Abgabenverwaltung und der Sozialversicherung (VfGH 2. Oktober 2006, G 29/06, V 18/06).

3.2. Im Hinblick auf den Ausgangspunkt des Eingriffs trifft § 1 Abs. 2 eine grundlegende Unterscheidung: Während bei Eingriffen von Privaten die Abwägung im Einzelfall unmittelbar auf Grund von § 1 Abs. 2 stattfinden kann, ist für Eingriffe einer staatlichen Behörde zusätzlich Voraussetzung, dass sie auf Grund von Gesetzen erfolgen, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind. § 1 Abs. 2 enthält also einen materiellen Gesetzesvorbehalt (VfSlg. 16.150/2001) für **Eingriffe durch staatliche Behörden**. Das Vorliegen einer gesetzlichen Grundlage – als formellem Kriterium – reicht demgemäß alleine nicht aus, den Eingriff zu legitimieren.

3.3. Die Unterscheidung zwischen Eingriffen Privater und staatlicher Behörden ist freilich nur eine relative: Denn einerseits schließt § 1 Abs. 2 es nicht aus, auch Eingriffe Privater durch Gesetz näher zu regeln und damit die Interessenabwägung vom Einzelfall zu abstrahieren (dies tut schon das DSG 2000, etwa in § 8 Abs. 3 Z 4 und 5 sowie § 9 Z 9; im Einzelfall kann dies sogar geboten sein, vgl. unten Pkt. 7.3.) und muss sich auch die unmittelbare

Interessenabwägung an Maßstäben aus der Rechtsordnung orientieren (arg. „berechtigt“), andererseits muss die für behördliche Eingriffe notwendige gesetzliche Grundlage nicht immer eine „ausdrückliche“ gesetzliche Regelung sein, sondern können derartige gesetzliche Regelungen auch auf Grund von Generalklauseln im Zusammenhalt mit anderen Rechtsvorschriften erfolgen (s. dazu sogleich).

4. Ausdrückliche gesetzliche Regelungen

4.1. Aus den Materialien zu den Vorgängerbestimmungen von § 8 Abs. 1 Z 1 und § 9 Z 3 DSG 2000 im DSG 1978 ergibt sich, dass diese Bestimmungen als Auftrag an den jeweils zuständigen Gesetzgeber zu verstehen sind, nach und nach bereichsspezifische Datenschutzbestimmungen und damit eine dem Art. 18 Abs. 1 B-VG besser (als eine Generalklausel) entsprechende Verrechtlichung des EDV-Einsatzes zu schaffen (näher *Dohr/Pollirer/Weiss*, DSG², § 8, Anm. 5). Eine solche Bestimmung soll enthalten

- Anlass und Zweck der Verwendung (§ 4 Z 8),
- die von der Verwendung Betroffenen (§ 4 Z 3),
- die Kategorien der zu verwendenden Datenarten (§ 4 Z 1),
- den oder die Auftraggeber (§ 4 Z 4),
- allfällige Übermittlungsempfänger (§ 4 Z 12),
- Angaben über technisch-organisatorische Besonderheiten der Verwendung (wie z.B. Speicherung der Daten in einem Register, Verarbeitung der Daten in einem Informationsverbundsystem [§ 4 Z 13], Möglichkeit von online-Zugriffen etc.).

Die Generalklausel des § 8 Abs. 3 Z 1 gilt nur für die Verwendung nicht-sensibler Daten. Gesetze, die gemäß § 1 Abs. 2 iZm § 9 Z 3 erlassen werden, erst recht eine entsprechend genaue **Determinierung** enthalten müssen. S. zu den sensiblen Daten auch unten Pkte. 5.2. und 7.

4.2. Aufmerksam gemacht wird auch auf § 12 Abs. 3 Z 3, wonach die Übermittlung oder Überlassung von Daten ins Ausland genehmigungsfrei ist, wenn sie gesetzlich vorgesehen ist. Eine entsprechende Anordnung muss freilich § 1 Abs. 2 entsprechen.

4.3. Generelle Umschreibungen, wie die Pflicht „Auskünfte zu erteilen, die für den Vollzug dieses Gesetzes und der relevanten internationalen Vorschriften notwendig sind“ (§ 83 Abs. 2 TKG 2003), allein stellen „angesichts der Weite

[dieser] Ermächtigung, Auskünfte zu verlangen, kein nach § 1 Abs. 2 DSG 2000 iVm Art. 8 Abs. 2 EMRK notwendiges, Eingriffe in das Grundrecht auf Datenschutz legitimierendes Gesetz“ dar (VfSlg. 16.369/2001). Regelungen, die keine über § 8 Abs. 3 Z 1 hinausgehende Konkretisierung enthalten, sind im Übrigen auch schon aus rechtssystematischen Überlegungen zu vermeiden.

5. Generalklausel

5.1. § 8 Abs. 3 Z 1 stellt eine **Generalklausel** dar, wonach schutzwürdige Geheimhaltungsinteressen nicht verletzt sind, wenn die Verwendung der Daten für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist. Dies setzt voraus, dass die Aufgaben des Auftraggebers des öffentlichen Bereichs im Gesetz klar umschrieben sind und klare Rückschlüsse auf damit verbundene Datenverwendungen möglich sind. Wichtig ist, dass die **Zusammenschau der in den Materiengesetzen enthaltenen Regelungen mit den allgemeinen Grundsätzen über die Verwendung von Daten gemäß Art. 2 (= §§ 4 ff) DSG 2000** eine im Auslegungsweg ermittelbare, **hinreichend präzise Regelung** darstellt. Dies freilich nur unter der Voraussetzung, dass die sich daraus ergebenden Grenzen der Datenerhebung und -verwendung § 1 Abs. 2 letzter Satz zufolge nach Maßgabe des Verhältnismäßigkeitsgrundsatzes bestimmt werden, sodass „der Eingriff in das Grundrecht nur in der gelindesten, zum Ziel führenden Art vorgenommen“ wird. (vgl. VfGH 15. Juni 2007, G 147/06 ua zur „Section Control“). Das Absehen von einer „ausdrücklichen gesetzlichen Ermächtigung“ wird insbesondere dann zulässig sein, wenn eine genaue Determinierung der zu verwendenden Datenarten gar nicht möglich ist.

5.2. Die (gegenüber § 8 Abs. 3 Z 1) unterschiedliche Formulierung des § 9 Z 3 verdeutlicht die schon in § 1 Abs. 2 zu Grunde gelegten strengeren Anforderungen für die Verwendung sensibler Daten im Hinblick auf die Determinierung und die Erforderlichkeit des Eingriffs: Die Anordnung der Datenverwendung muss sich aus dem Gesetz unzweifelhaft ergeben, das wichtige öffentliche Interesse daran wäre in den Erläuterungen darzulegen. Derartige Regelungen sollten also möglichst „ausdrücklich“ im Sinn von Pkt. 4.

sein (beachte freilich auch Pkt. 5.6. und die sogleich unter 5.3. folgenden Beispiele).

5.3. In VfSlg. 12.166/1989 hat der VfGH die Vorgängerbestimmung von § 8 Abs. 3 Z 1 DSG 2000 – nämlich § 7 Abs. 2 DSG 1978 – iVm § 20 VfGG als notwendig »*"zum Schutz der Rechte und Freiheiten anderer", nämlich des - Rechtsschutz suchenden – Beschwerdeführers*« erkannt. In VfSlg. 15.130/1998 war der VfGH der Ansicht, dass die Aufgabenübertragung an den Rechnungshof durch Art 127a B-VG für sich alleine betrachtet schon eine ausreichende (verfassungs-)gesetzliche Grundlage zur Datenverwendung darstelle und keiner weiteren Konkretisierung bedürfe. Dies ist im Hinblick auf VfSlg 17.065/2003 grundsätzlich auch für sensible Daten anzunehmen, wenngleich sich Einschränkungen aus dem Verhältnismäßigkeitsgrundsatz ergeben können.

5.4. Die beiden zuvor genannten Erkenntnisse sind im Lichte der EGMR-Judikatur zu verstehen: Im Urteil *Rekvenyi* gegen *Ungarn* vom 20. Mai 1999, Appl. 25390/94 (ÖJZ 2000, 235), hat der EGMR in Rz 34 festgehalten, dass *der Grad an Genauigkeit, der von der innerstaatlichen Gesetzgebung - welche nicht in jedem Fall für jede Eventualität Sorge tragen kann - verlangt wird, in einem beträchtlichen Ausmaß vom Inhalt des in Rede stehenden Instruments, dem vorhergesehenen Anwendungsbereich und der Anzahl und dem Status derjenigen abhängt, an die es sich richtet*.

5.5. Nach Ansicht des Bundeskanzleramtes-Verfassungsdienst liegen beiden unter 5.3. genannten Fällen Sachverhalte zu Grunde, in denen die präzise Aufzählung von Datenarten kaum möglich ist. Denn weder in einem Verfahren vor dem VfGH noch im Rahmen der Prüfungstätigkeit des Rechnungshofs kann im Vorhinein zweifelsfrei festgestellt werden, welche Daten tatsächlich benötigt werden. Das wird generell für Datenermittlungen im Zuge von Verfahren anzunehmen sein (s. dazu den Bescheid der Datenschutzkommission vom 29. November 2006, GZ K121.229/0006-DSK/2006).

5.6. In Fällen der faktischen Unmöglichkeit der Schaffung einer ausdrücklichen gesetzlichen Regelung wird jedenfalls darauf zu achten sein, dass im Sinne des § 8 Abs. 3 Z 1 eine möglichst genaue Umschreibung der Aufgaben eines Auftraggebers des öffentlichen Bereichs erfolgt, die klare Rückschlüsse auf die Zulässigkeit der Verwendung von Daten ermöglicht. Dies zeigt, dass die

Unterscheidung zwischen ausdrücklicher gesetzlicher Regelung (§ 8 Abs. 1 Z 1) und (§ 8 Abs. 3 Z 1 präzisierender) Generalklausel in manchen Fällen fließend ist.

## 6. Notwendige gesetzliche Beschränkungen – Verhältnismäßigkeit

6.1. Eingriffe in das Grundrecht auf Datenschutz müssen verhältnismäßig sein. Aus der Judikatur des VfGH hat die Lehre (vgl. *Berka*, Die Grundrechte, Rz 266 ff) folgende Kriterien der **Verhältnismäßigkeit** herausgearbeitet:

- Der mit dem Eingriff verfolgte Zweck muss legitim sein.
- Der Eingriff muss zur Zielerreichung geeignet und darüber hinaus
- erforderlich sein.
- Außerdem muss ein zwischen dem durch den Eingriff zu erreichenden Zweck und der Art des Eingriffs ein angemessenes Verhältnis bestehen (Verhältnismäßigkeit im engeren Sinn).

6.2. Als besondere Betonung der Verhältnismäßigkeit sieht § 1 Abs. 2 letzter Satz das **Gebot des gelindesten Mittels** vor. Für die legistische Gestaltung von Eingriffsermächtigungen bedeutet dies, dass erstens unter mehreren geeigneten und erforderlichen Mitteln nur jenes mit der geringsten Eingriffsintensität verfassungsrechtlich zulässig ist (§ 1 Abs. 2 letzter Satz) und zweitens auch dieses gelindeste Mittel insgesamt in einem angemessenen Verhältnis zum angestrebten Zweck stehen muss.

6.3. Nach der Judikatur des VfGH sind insbesondere **notwendig**:

- die Aktenvorlage durch belangte Behörden an den VfGH, um die Effizienz des Rechtsschutzes gewährleisten zu können (VfSlg. 12.166/1989);
- die Erhebung von Wirtschaftsdaten für Zwecke der Wirtschaftsforschung und in weiterer Folge der Wirtschaftspolitik für das wirtschaftliche Wohl eines Landes (VfSlg. 12.228/1989);

6.4. Als **nicht notwendig** iSd Art. 8 Abs. 2 EMRK und daher verfassungswidrig bzw. richtlinienwidrig hat der VfGH erachtet:

- die namentliche Registrierung von Videothekbenützern für Zwecke der Besteuerung, da die Einhebung einer Vergnügungssteuer auch ohne Identitätsfeststellung des Mieters möglich ist (VfSlg 12.689/1991);
- die Bestimmung des § 83 Abs. 2 TKG, wonach Konzessionsinhaber dem Bundesminister alle Auskünfte zu erteilen hätten, die für den Vollzug

dieses Gesetzes und der relevanten internationalen Vorschriften notwendig seien – die Notwendigkeit scheiterte aus Sicht des VfGH an der Weite der Bestimmung (VfSlg 16.369/2001); die Beschränkung des – ebenfalls verfassungsgesetzlich (§ 1 Abs. 3 Z 1) gewährleisteten – Auskunftsrechts auf die Aufbewahrungsdauer sowie die Löschungsmöglichkeiten der gespeicherten erkennungsdienstlichen Daten, somit den Ausschluss der Beauskunftung der Datenarten und der anderen nach dem DSG 2000 vorgesehenen Auskunftsinhalte durch eine einfachgesetzliche Bestimmung des Sicherheitspolizeigesetzes (VfSlg. 16.986/2003);

- die namentliche Veröffentlichung von Bezügeempfängern zur „*sparsamen und effizienten Verwendung öffentlicher Mittel*“ – die wohl auch auf den Eingriffstatbestand des „*wirtschaftlichen Wohl des Landes*“ (Art. 8 Abs. 2 EMRK) zurückzuführen wäre –, weil andere, weniger eingriffsintensive Vorgangsweisen ebenso zielführend sind (VfSlg. 17.065/2003).

6.5. Beispiel:

Soll verhindert werden, dass gefährliche Tiere (Schlangen, Spinnen, etc. …) von Personen gehalten werden, die aus bestimmten Gründen nicht vertrauenswürdig erscheinen, so wäre eine Datenbank aller Haustiere mit Verknüpfung der Tierhalter und deren vollständiger Strafkartei, sowie eine Historisierung dieser Daten und umfangreiche Zugriffsmöglichkeiten durch andere Stellen aus den folgenden Gründen nicht im Einklang mit § 1 Abs. 2:

- Erstens würde es genügen, nur die gefährlichen Tiere und deren Halter in die Datenbank aufzunehmen (Gebot des gelindesten Mittels).
- Zweitens erscheint selbst eine Datenbank der gefährlichen Tiere, die auch eine Verknüpfung mit Strafdaten des Halters beinhaltet, immer noch als unverhältnismäßig, da beispielsweise der Zugriff durch Dritte auf die Strafdaten nicht erforderlich ist. Vielmehr genügte es, in einem Verfahren die Vertrauenswürdigkeit des potentiellen Tierhalters festzustellen und ihm darüber eine Bestätigung auszustellen, mit der er solche Tiere erwerben darf.

## 7. Besondere Formerfordernisse bei der Verwendung sensibler Daten

7.1. Art. 8 Abs. 1 DS-RL verbietet grundsätzlich die Verwendung sensibler Daten, wovon Abs. 2 folgende Ausnahmetatbestände vorsieht:

a. Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden; oder

b. die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist; oder

c. die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; oder

d. die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, daß sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden; oder

e. die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

7.2. Art. 8 Abs. 3 DS-RL sieht Ausnahmen für die Fälle vor, in denen die Verarbeitung von Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

7.3. Art. 8 Abs. 4 DS-RL erlaubt den Mitgliedstaaten, diese Ausnahmetatbestände zu erweitern, sofern diese Erweiterungen auf einer gesetzlichen Grundlage oder der Entscheidung der nationalen Kontrollstelle (dh der Datenschutzkommission) beruhen. Voraussetzung dafür ist allerdings, dass angemessene Garantien vorgesehen werden. Da eine Entscheidung der Datenschutzkommission im Hinblick auf Art. 18 Abs. 1 B-VG stets auf einem Gesetz beruhen muss, ist in Österreich stets eine hinreichend determinierte gesetzliche Grundlage erforderlich.

7.4. Im Gegensatz zur Regelung der **Verwendung nicht-sensibler Daten** ist daher **auch bei Eingriffen durch Private eine gesetzliche Regelung** als Rechtsgrundlage notwendig, wenn es zur Verwendung sensibler Daten kommen soll und nicht einer der in Art. 8 Abs. 2 oder 3 DS-RL angeführten Ausnahmetatbestände zum Tragen kommt.

7.5. Gemäß § 1 Abs. 2 DSG 2000 darf die Verwendung von „Daten die ihrer Art nach besonders schutzwürdig sind“ (das sind sensible Daten iS des § 4 Z 2) nur zur Wahrung wichtiger öffentlicher Interessen vorgesehen werden und müssen derartige Gesetze gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen.

7.6. Unter den in Art. 8 Abs. 4 (und 5, s. sogleich Pkt. 8.) DS-RL bzw. § 1 Abs. 2 DSG 2000 vorgesehenen **angemessenen Garantien** können verstanden werden (wobei diese je nach Intensität des geplanten Eingriffs auch kumuliert vorgesehen werden sollten):

a. strenge Datensicherheitsmaßnahmen wie etwa die lückenlose Zugriffsprotokollierung oder die Verschlüsselung der Daten,

b. besondere Verschwiegenheitspflichten etwa in Bereichen, in denen die Amtsverschwiegenheit oder andere spezielle Verschwiegenheits-pflichten wie etwa jene von Ärzten nicht greifen,

c. ausdrückliche Verwendungsbeschränkungen bzw. -verbote[2]

d. besondere Informationsverpflichtungen;

e. besondere Rechtsschutzmechanismen.

7.7. Gemäß § 54 Abs. 1 DSG 2000 hat der Bundeskanzler von der Erlassung eines Bundesgesetzes, das die Zulässigkeit der Verarbeitung sensibler Daten betrifft, anlässlich der Kundmachung des Gesetzes im Bundesgesetzblatt der Europäischen Kommission Mitteilung zu machen. In richtlinienkonformer Interpretation bezieht sich diese Verpflichtung auf die in Art. 8 Abs. 4 DS-RL erlaubten Abweichungen von Art. 8 Abs. 1 DS-RL (s. oben die Pkte. 7.3. bis 7.6.). Die Wahrnehmung dieser Notifizierungspflicht setzt voraus, dass der Bundeskanzler (schon anlässlich der Begutachtung derartiger Gesetze) auf diesen Umstand aufmerksam gemacht wird. Ein derartiger Hinweis sollte sich ausdrücklich im **allgemeinen Teil der Erläuterungen** bzw. im **Ausschussbericht** finden.

## 8. Strafrechtlich relevante Daten

Grundsätzlich gilt für die Verwendung derartiger Daten (worunter auch Daten im Zusammenhang mit Verwaltungsübertretungen fallen) das unter Punkt 4. bis 6. Gesagte. Es ist aber darauf hinzuweisen, dass die Verwendung

2 Vgl. WP 83 der Artikel 29 Datenschutzgruppe, 7, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp83_de.pdf (27.11.2007).

strafrechtlich relevanter Daten durch die Regelung in Art. 8 Abs. 5 DS-RL in die Nähe der sensiblen Daten gerückt wird, weshalb auch hier besonders auf eine ausreichende gesetzliche Determinierung zu achten sein wird. Auf die Sonderbestimmung des § 8 Abs. 4 DSG 2000 wird hingewiesen.

## 9. Zulässigkeit von Eingriffsermächtigungen im Verordnungsrang

9.1. „Eingriffsermächtigungen“ im Verordnungsrang stellen für sich alleine **keine taugliche Eingriffsermächtigung** iSd § 1 Abs. 2 dar, weil dieser ein Gesetz im formellen Sinn erfordert. Ein Eingriff in das Recht auf Geheimhaltung muss sich daher aus einem solchen ableiten lassen. Jedenfalls auch datenschutzrechtlich unzulässig ist daher eine formalgesetzliche Delegation von Eingriffsermächtigungen an den Verordnungsgeber.

9.2. Dennoch sind Fälle denkbar, in denen Verordnungen zulässigerweise Eingriffsermächtigungen konkretisieren, weil die Intensität des Eingriffs bereits abschließend im Gesetz vorgezeichnet ist. Im Wesentlichen ist hier auf das Verhältnis von Gesetz und Verordnung im Lichte des Art. 18 Abs. 1 B-VG zu verweisen. Insbesondere können auch Generalklauseln (oben 5.) durch Verordnung konkretisiert werden. Für unbedenklich (im konkreten Fall sogar geboten) hat der VfGH etwa die verordnungsmäßige Festlegung jener Wegstrecken erachtet, auf denen eine so genannte „section control“ (automationsunterstützte Geschwindigkeitskontrolle, die im Überschreitungsfall zur weiteren Verwendung der Daten des KFZ-Halters führt) erfolgen soll (Erk. G 147/06 ua. s. bereits oben 5.1.).

9.3. Nicht ausgeschlossen ist insbesondere auch eine Präzisierung durch die Aufzählung von Detaildatenarten, die den Rahmen eines Gesetzes sprengen würden. Beispielsweise wären in einem Gesetz die Datenarten, die ein Ausweis enthalten muss, zu regeln. Die nähere Ausgestaltung des Ausweises (Format, dgl.) kann in Verordnungsrang geregelt werden (vgl. zB das Verhältnis zwischen § 3 des Passgesetzes und der PassV).

## 10. Informationsverbundsysteme

Sollen durch Gesetz Informationsverbundsysteme im Sinne von § 4 Z 13 geschaffen werden, so wäre im Gesetz insbesondere die Rollenverteilung zu regeln (wer ist Auftraggeber, wer ist Dienstleister, wer ist Betreiber des Systems). Als Beispiele für im öffentlichen Bereich geregelte

Informationsverbundsysteme sind insbesondere das Zentrale Melderegister (§ 16 MeldeG) und die in den §§ 57 ff SPG geregelte Zentrale Informationssammlung der Sicherheitsbehörden zu nennen.

## 11. Einheitliche Begriffsbildung

11.1. In Erinnerung gerufen wird zunächst Pkt. 31 der Legistischen Richtlinien 1990, wonach auf einen einheitlichen Sprachgebrauch nicht nur innerhalb der zu erlassenden Norm, sondern soweit dies möglich ist, innerhalb der gesamten Rechtsordnung zu achten ist.

11.2. Soweit datenschutzrechtlich relevante Regelungen ausgearbeitet werden, sollte daher unbedingt die Terminologie des DSG 2000 herangezogen werden, um Auslegungsprobleme hintanzuhalten. Datenschutzrechtliche Relevanz besteht bei der Verwendung von Angaben über Betroffene (§ 4 Z 3 DSG 2000) – nicht jedoch, wenn Daten verwendet werden, die nicht auf Betroffene rückführbar sind. Trotzdem wäre es auch in diesen Fällen sinnvoll die Begriffe des DSG 2000, wie etwa „übermitteln“ an Stelle von „schicken“, „senden“ oder dergleichen zu verwenden.

11.3. Die folgenden Beispiele betreffen typische terminologische Fehlgriffe:

| **Statt** | **Besser** |
|---|---|
| *Datenverarbeiter* oder *Person, die für die Datenverwendung zuständig ist* | Auftraggeber (§ 4 Z 4 DSG 2000) |
| *Gehilfe* oder *Subunternehmen* | Dienstleister (§ 4 Z 5 DSG 2000) |
| *schicken*, *senden*, *weiterleiten* oder *mitteilen* | übermitteln (§ 4 Z 12 DSG 2000) |
| *übermitteln, weiterleiten, schicken, senden* oder *übergeben von Daten an den Dienstleister* | überlassen (§ 4 Z 11 DSG 2000) |
| *verarbeiten* (wenn auch die Übermittlung umfasst sein soll) | verwenden (§ 4 Z 8 DSG 2000) |
| *Information* (sofern personenbezogen) | Daten (§ 4 Z 1 DSG 2000) |
| *Einwilligung, Zustimmungserklärung* oder *Einverständnis* | Zustimmung (§ 4 Z 14 DSG 2000) |

## 12. Verhältnis zu früheren Rundschreiben

Rundschreiben, die sich auf Bestimmungen des alten Datenschutzgesetzes (DSG), BGBl. Nr. 565/1978 beziehen, sind bereits mit dem Wegfall ihrer gesetzlichen Grundlage – sprich der Aufhebung des DSG durch das DSG 2000 mit Wirkung vom 1. Jänner 2000 – gegenstandslos geworden. Insbesondere gilt dies für:

- das Rundschreiben vom 26. Juni 1980, GZ 810.016/1-V/3/80,
- das Rundschreiben vom 1. Juni 1981, GZ 810.090/1-V/3/81,
- das Rundschreiben vom 21. April 1982, GZ 810.099/4-V/4/81 und
- das Rundschreiben vom 18. März 1985, GZ 810.099/1-V/1a/85.

14. Mai 2008
Für den Bundeskanzler:
Georg LIENBACHER

***Elektronisch gefertigt***