REPUBLIK ÖSTERREICH
DATENSCHUTZRAT

A-1014 Wien, Ballhausplatz 1
Tel. (0222) 6615/2528, 2525
Fernschreib-Nr. 1370-900

531 15/O

GZ 816.082/3-DSR/90

Dr. WETTER
2544

Regierungsvorlage zum
Sicherheitspolizeigesetz;

Stellungnahme des Datenschutzrates

An das
Präsidium des Nationalrates

Parlament
1010 W i e n

Der Datenschutzrat übermittelt in der Beilage die gegenüber dem Bundesministerium für Inneres abgegebene Stellungnahme zur Regierungsvorlage zum Sicherheitspolizeigesetz sowie die am 19. April 1990 und teilweise noch aufrechterhaltene Stellungnahme zum Ministerialentwurf, jeweils in 25-facher Ausfertigung.

Beilagen

2. Oktober 1990
Für den Datenschutzrat
Der Vorsitzende:
i.A. DOHR

Für die Richtigkeit
der Ausfertigung:

REPUBLIK ÖSTERREICH
DATENSCHUTZRAT

A-1014 Wien, Ballhausplatz 1
Tel. (0222) 6615/2528 2525
Fernschreib-Nr. 1370-900

531 15/O

GZ 816.028/3-DSR/90

Dr. SINGER
2768

Sicherheitspolizeigesetz -
Erkennungsdienstgesetz,
Begutachtungsverfahren;

Stellungnahme des Datenschutzrates

An das
Bundesministerium für Inneres

Postfach 100
1014 W i e n

Der Datenschutzrat hat in seiner Sitzung am 30. März 1990 zu dem mit do. Zl. 112 777/15-I/7/90 vom 23. Februar 1990 übermittelten Entwurf eines Sicherheitspolizeigesetzes sowie zum Entwurf eines Erkennungsdienstgesetzes (3. Abschnitt des Sicherheitspolizeigesetzes) und zu dem ikW übermittelten Entwurf eines § 40a Sicherheitspolizeigesetz beschlossen, folgende Stellungnahme abzugeben:

I. Allgemeines:

Der Datenschutzrat empfiehlt, die vorgesehenen Bestimmungen über den Datenschutz im Sicherheitspolizeigesetz entsprechend den Beratungen des Datenschutzrates in seiner Sitzung am 30. März 1990, an der auch zwei Vertreter des Bundesministeriums für Inneres teilnahmen, einer Prüfung zu unterziehen und gegebenenfalls Änderungen im Sinne der Aufrechterhaltung des Zweckes des Datenschutzgesetzes vorzunehmen.

Der Datenschutzrat nimmt mit Genugtuung zur Kenntnis, daß das Auskunftsrecht für alle ermittelten und verarbeiteten personenbezogenen Daten Anwendung finden soll (§ 40 a).

Generell ist zu diesem Entwurf zu sagen, daß jegliche Übergangsbestimmungen fehlen. Es fehlt weiters die Bedachtnahme auf die Regelungen des Datenschutzgesetzes in jenem Abschnitt des Gesetzes, welcher den Rechtsschutz behandelt. Schließlich müßte geklärt werden, was mit jenen Daten zu geschehen hat, die bisher entgegen den Regelungen des Datenschutzgesetzes gespeichert, verwendet etc. wurden. Diese Daten wären entweder einer besonderen Überprüfung zu unterziehen oder überhaupt zu löschen. Schließlich wäre der gesamte Gesetzesentwurf auch in formeller Hinsicht dem Datenschutzgesetz anzugleichen. So ist beispielsweise die vom § 37 des Entwurfes eröffnete Wahlmöglichkeit zwischen gesetzlichen Ermächtigungen einerseits und generellen Aufträgen andererseits nicht mit dem Grundgedanken des Datenschutzgesetzes vereinbar.

II. Zum Entwurf eines Sicherheitspolizeigesetzes:

Zu § 36: Der Terminus "Verwenden" ist von § 3 Z 12 des DSG als Ermitteln, Verarbeiten, Benützen, Übermitteln und Überlassen von Daten oder einem dieser Vorgänge definiert. Nach § 36 des Entwurfes ist auch das Ermitteln und Verarbeiten von Daten zulässig, soweit dies zur Erfüllung der den Sicherheitsbehörden auf dem Gebiet der Sicherheitspolizei übertragenen Aufgaben erforderlich ist. Damit geht diese Regelung jedoch hinsichtlich des Ermittelns und Verarbeitens über die wesentlich strengere Regelung des § 37 Abs. 1 des Entwurfes hinaus und bewirkt dessen Wirkungslosigkeit. Da der Entwurf spezielle Ermittlungs-, Verarbeitungs- und Übermittlungsregelungen enthält, ist daher eher davon auszugehen, daß mit § 36 das "Benützen von Daten" geregelt ist (vgl. § 3 Z 8 DSG) sohin jede Form der Handhabung von Daten einer Datenverarbeitung, die nicht Ermitteln, Verarbeiten oder Übermitteln ist. Eine terminologische Klarstellung wäre unerläßlich. Zusätzlich wäre anzuführen, daß diese Daten nur dann benützt werden dürfen, soweit sie zur Erfüllung der den Sicherheitsbehörden auf dem Gebiet der Sicherheitspolizei übertragenen Aufgaben in konkreten Fällen eine wesentliche Voraussetzung sind.

Zu § 37 Abs. 1: § 37 Abs. 1 ist lediglich eine Wiedergabe der Regelung des § 6 DSG. Die demonstrative Aufzählung der gesetzlich übertragenen Aufgaben ändert daran nichts. Vorzuziehen wäre eine taxative Aufzählung der gesetzlich übertragenen Aufgaben.

Zu Z 2 und 3 ist anzumerken, daß die darin vorgesehene Regelung derart unbestimmt ist, daß eine verfassungskonforme Vollziehung kaum möglich erscheint. Es ist nicht festgelegt, welche Kriterien vorliegen müssen, damit die Ermittlung und Verarbeitung von Daten zur Vorbeugung eines Angriffes zulässig ist. Im Hinblick auf die verfassungsrechtlichen Garantien der Privatsphäre und das Gebot, Eingriffe auf ein absolut notwendiges Minimum zu beschränken, ist es erforderlich, konkrete Verdachtsmomente zu verlangen. Darüberhinaus wäre es erforderlich, jene öffentlichen Interessen, die einen Eingriff in das Grundrecht auf Datenschutz im Sinne des § 1 Abs. 2 DSG rechtfertigen sollen, unter Bezugnahme auf jene Rechtsgüter zu umschreiben, die Art. 8 Abs. 2 EMRK nennt, um die Verfassungskonformität dieser Bestimmung zu gewährleisten.

Zu § 37 Abs. 2: § 3 Z 9 DSG definiert die Datenübermittlung u.a. als die Verwendung von Daten für ein anderes Aufgabengebiet desselben Auftraggebers. Ein derartiger Fall liegt hier vor. Abgesehen davon, daß diese Bestimmung, die gleichzeitig eine Ermittlungsermächtigung für die Sicherheitsbehörden ist, in systemwidrigem Gegensatz zu § 37 Abs. 1, der wesentlich strengere Voraussetzungen für die Ermittlung und Verarbeitung vorsieht, steht, ist diese Bestimmung auch datenschutzrechtlich und verfassungsrechtlich bedenklich. Die Erläuterungen zu dieser Bestimmung vermögen nicht überzeugend klarzulegen, warum ohne gesetzlich verankerte weitere Beschränkung eine generelle Ermächtigung bestehen sollte, Daten aus anderen Verwaltungsgebieten für Zwecke, die im § 37 Abs. 1 genannt (dort aber nur beispielhaft aufgezählt sind) zu verarbeiten. Eine derartige generelle Ermächtigung widerspricht dem Grundgedanken des Datenschutzgesetzes, wonach

Daten ausschließlich für konkrete Aufgaben verwendet werden dürfen. Sollte die Bestimmung jedoch so zu verstehen sein, daß die Daten nur im Zusammenhang mit konkreten Fällen herangezogen, also übermittelt werden dürfen, bietet der Gesetzestext hierfür keine Anhaltspunkte. Darüber hinaus ergäbe sich diese Möglichkeit bereits aus § 7 Abs. 2 DSG.

37(4)

Zu § 37 Abs. 3: Es ist unklar, was unter "Dienststellen der Gebietskörperschaften" zu verstehen ist. Sowohl Art. 22 B-VG als auch § 7 Abs. 2 DSG verwenden im Rahmen der Amtshilfe den Begriff "Organ". Es wäre daher sinnvoll, sich an diesen Bestimmungen zu orientieren.

Die Beschränkung auf die im zweiten Halbsatz aufgezählten Datenarten ist grundsätzlich zu begrüßen. Es wäre jedoch klarzustellen, daß daraus nicht abgeleitet werden darf, daß diese Datenarten jedenfalls zu übermitteln sind. Diese Aufzählung kann lediglich der Maximalumfang sein. Gegenstand der Übermittlung dürfen nur jene Daten sein, die für die Abwehr und Aufklärung von schwerwiegenden Angriffen gemäß § 37 Abs. 1 Z 2 und Z 3 unbedingt benötigt werden. Eine Klarstellung, was unter "schwerwiegend" zu verstehen ist, wäre notwendig.

37/5

Zu § 37 Abs. 4: Auch diese Datenübermittlungen sollen global und ohne Bezugnahme auf konkrete Verdachtsmomente erfolgen. Ein Eingriff in das Grundrecht auf Datenschutz kann nur dann verfassungsrechtlich unbedenklich sein, wenn es zur Erreichung bestimmter öffentlicher Interessen notwendig ist. Dies setzt in aller Regel einen konkreten Anlaßfall voraus. Die Erläuterungen enthalten keine ausreichenden Hinweise darauf, daß bei konkreten Verdachtsmomenten für die Verletzung von Umweltauflagen diese Informationen nicht auch im Einzelfall angefordert werden können.

Zu § 38 Abs. 1 Z 2: Eine Speicherung ist nur dann zulässig, wenn der ausländische richterliche Befehl auch im Inland Rechtswirkungen hat. Der Hinweis der Erläuterungen auf das

Auslieferungs- und Rechtshilfegesetz geht insoweit ins Leere, als nach dieser Bestimmung eine Auslieferung etwa wegen Verletzung von Abgaben-, Monopol-, Zoll- oder Devisenvorschriften, aber auch in einer Reihe anderer Fälle von vornherein unzulässig wäre.

Zu § 38 Abs. 2: Den Erläuterungen zu dieser Bestimmung ist zu entnehmen, daß die in derartige Datenverarbeitungen aufzunehmenden Daten dem Zweck der Sachenfahndung, also der Fahndung nach Kulturgut, Schmuck oder anderen identifizierbaren Sachen dienen. Diese Zielsetzung sollte klarer im Gesetzestext hervorkommen. Es erscheint jedoch verfassungsrechtlich bedenklich, im Rahmen einer Sachenfahndung ein Verzeichnis solcher Personen anlegen zu wollen, welche an Hand nicht näher determinierter Kriterien als potentielle Straftäter eingeschätzt werden. Voraussetzung für die Ermittlung und Verarbeitung von Daten bleibt jedenfalls die unmittelbare konkrete Gefahr.

Zu § 38 Abs. 4: Wie bereits ausgeführt, erfordert die Ermittlung und Verarbeitung von Daten das Vorliegen einer konkreten Berechtigung. Das sind im Zusammenhang mit der hier zu behandelnden Evidenz die im § 38 Abs. 1 genannten Fälle. Fallen diese Voraussetzungen weg, fehlt es auch an einer weiteren sachlichen Berechtigung für die Speicherung der Daten. Jedenfalls wären die Daten nach rechtskräftigem Abschluß eines gerichtlichen Strafverfahrens zu löschen. Die Argumente der Erläuterungen zu Z 1, warum nach Widerruf eines richterlichen Befehles die Speicherung zwei Jahre aufrecht bleiben soll (nämlich Entscheidungshilfe dafür, ob zu einem späteren Zeitpunkt wegen eines anderen Sachverhaltes aus einem der früheren Haftgründe ein Haftbefehl zu erteilen sei), überzeugen nicht. Zusätzlich erscheint das Erfordernis einer zweijährigen Speicherung von inländischen Haftbefehlen zweifelhaft, da bei ausländischen Haftbefehlen eine sofortige Löschung nach Widerruf zu erfolgen hat.

Zu Z 4 ist anzumerken, daß die Löschung jedenfalls nach rechtskräftiger Beendigung des Strafverfahrens zu erfolgen hätte. Für eine fünfjährige Speicherung fehlt jede sachliche Rechtfertigung.

Zu den in Z 5 genannten Fällen (fünf Jahre nach Auffinden eines Gesuchten) liegt ebenfalls keine ersichtliche sachliche Rechtfertigung vor. Der Zweck der Aufnahme dieser Daten in die Evidenz ist mit Auffinden der Person erreicht. Die Daten wären somit zu löschen.

Zu § 39 Abs. 1: Es wird auf die Bedenken zur Regelung des § 37 Abs. 2 verwiesen.

Zu § 39 Abs. 2 Z 3: Im Hinblick auf § 7 Abs. 1 Z 1 und Abs. 2 DSG scheint diese Bestimmung entbehrlich.

40/5

Zu § 39 Abs. 5: Diese Bestimmung sieht eine Richtigstellung von unrichtigen oder unvollständigen Daten dann vor, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist. Damit geht diese Bestimmung vom Ordnungssystem des § 12 DSG ab. § 12 Abs. 7 DSG sieht die Verständigung des Datenempfängers auf Verlangen des Betroffenen dann vor, soferne dieser ein berechtigtes Interesse glaubhaft macht und die Empfänger noch feststellbar sind. Im Gegensatz dazu verlangt § 39 Abs. 5 des Entwurfes den Beweis der Wahrung schutzwürdiger Interessen. Diese Abweichung entbehrt einer sachlichen Rechtfertigung und erscheint daher verfassungsrechtlich bedenklich.

Wenn begründet wird, daß bei Auskünften aus der zentralen Informationssammlung die Empfänger von einer Richtigstellung nicht verständigt werden können, da der erforderliche Verwaltungsaufwand unvertretbar groß wäre (was vom Datenschutzrat nicht überprüft werden kann), so wäre im Hinblick auf § 1 Abs. 2 DSG letzter Satz doch zu prüfen, ob nicht durch andere Maßnahmen ein Empfänger bei neuerlicher

Auskunft aus diesem Datensatz besonders auf die Richtigstellung dieser Daten aufmerksam gemacht werden könnte, indem etwa Richtigstellungen als solche besonders gekennzeichnet werden.

Zu § 40 Abs. 1: Diese Bestimmung muß nach Auffassung des Datenschutzrates so verstanden werden, daß "Aktualisierung" nicht "Richtigstellung" bedeutet, sondern lediglich die regelmäßige Fortschreibung eines Datensatzes umfaßt, da für Richtigstellungen ausschließlich § 40 Abs. 2 anzuwenden wäre. Es ist jedoch zu beachten, daß auch für die Aktualisierung die allgemeinen Ermittlungs- und Verarbeitungsermächtigungen vorliegen müssen. Fehlen diese Ermächtigungen für die als aktuellere Daten hinzuzufügenden Daten, so wären die ursprünglichen Daten - solange sie nicht als unrichtige Informationen richtigzustellen sind - unverändert zu belassen. Im Gegensatz dazu erlaubt Abs. 1 die Fortschreibung eines bestehenden Datensatzes ohne weitere Beschränkung.

Zu § 40 a: Der Datenschutzrat hält die Formulierung einer Auskunft, die sich auf Verarbeitungen im Sinne des § 4 Abs. 3 DSG beziehen, für verfehlt. In jenen Fällen, wo Daten verarbeitet wurden, müßte jedenfalls diese Tatsache mitgeteilt werden.

Zu Abs. 4 ist anzumerken, daß die dort vorgesehene neue Kompetenz der Datenschutzkommission mit den bisherigen, auch den Schutz verfassungsmäßiger Einrichtungen und Strafrechtspflege umfassenden Zuständigkeiten dieser Behörde zu harmonisieren wären, wobei keine Verschlechterung der Rechtsstellung des Betroffenen bewirkt werden dürfte. Die Regelungen des Datenschutzgesetzes sollten in diesem Entwurf stärker integriert werden.

III. Zum Entwurf eines Erkennungsdienstgesetzes (3. Abschnitt des Sicherheitspolizeigesetzes):

Zu § 1 Abs. 2 Z 6: Die Umschreibung "anderer technischer Maßnahmen" zur Identifikation einer Person ist unbestimmt. Die Identifikation einer Person ist das Ermitteln personenbezogener Daten und steht unter dem Grundrechtsschutz des § 1 DSG. Soferne technische Maßnahmen möglich sind, die einen Eingriff in die Persönlichkeitssphäre darstellen (zB. Überprüfung von Gewohnheiten etc.) wäre die Wahrung schutzwürdiger Interessen zu prüfen. Mangels konkreter inhaltlicher Ausgestaltung dieser Bestimmung kann daher deren Verfassungskonformität nicht beurteilt werden.

Zu § 1 Abs. 7: Die Bedeutung dieser Bestimmung ist unklar und wird auch durch die erläuternden Bemerkungen nicht erklärt. Es widerspräche jedoch dem Grundrecht auf Datenschutz, erkennungsdienstliche Maßnahmen ohne weitere Voraussetzung nach einer rechtskräftigen Verurteilung als zulässig zu erklären, da das Grundrecht auf Datenschutz eine Rechtfertigung in der Notwendigkeit, eine bestimmte Maßnahme zur Erreichung eines bestimmten öffentlichen Interesses zu setzen, verlangt.

Zu § 2 Abs. 2: Nach dieser Bestimmung wäre eine erkennungsdienstliche Behandlung jedenfalls zulässig, wenn zu befürchten ist, die Person werde weitere, mit Strafe bedrohte Handlungen begehen. Dieser Bestimmung fehlt eine Rücksichtnahme auf den Verhältnismäßigkeitsgrundsatz des § 1 Abs. 2 DSG. Wohl verweisen die Erläuterungen auf den Bereich der mittleren und schweren Kriminalität, ziehen aber keine Grenze zur leichten Kriminalität. Für die Beurteilung der Verhältnismäßigkeit dieser Bestimmung wäre es erforderlich, Kriterien anzugeben, an Hand derer eine Rückfallgefahr erkennbar ist. Es sollte daher der in den Erläuterungen ausgedrückte Gedanke in das Gesetz übernommen werden, daß Indizien dafür vorliegen müssen, daß Rückfallgefährlichkeit besteht. Nur in solchen Fällen sollte daher eine erkennungsdienstliche Behandlung zulässig sein. Es

wäre überdies auch auf die Deliktsart Bedacht zu nehmen. Solche Delikte, bei denen der Täter regelmäßig auf frischer Tat betreten wird (beispielsweise Ladendiebstahl) erfordern nach Auffassung des Datenschutzrates selbst bei Rückfallgefährlichkeit keine erkennungsdienstliche Behandlung, da das für die Strafbemessung relevante strafrechtliche Vorleben dem Strafregister entnehmbar ist.

Zu § 2 Abs. 3, Abs. 6 und 7: Der Verhältnismäßigkeitsgrundsatz des Grundrechtes auf Datenschutz verlangt, daß ein Grundrechtseingriff durch das gelindeste Mittel erfolgt. Da diese Bestimmung bei zweifelhafter Identität jedenfalls eine erkennungsdienstliche Behandlung zuläßt, ist sie unverhältnismäßig, da sie nicht darauf Bedacht nimmt, daß auch andere Möglichkeiten der Identitätsfeststellung (zB. Ausweiskontrollen, Gegenüberstellungen) möglich wären. Die erkennungsdienstliche Behandlung darf nur die ultima ratio für die Feststellung der Identität sein. Soferne daher andere, weniger grundrechtseinschränkende Möglichkeiten zur Identitätsfeststellung gegeben sind, sind diese zu wählen.

Zu § 4 Abs. 1: Diese Bestimmung erlaubt unter der Voraussetzung, daß die erkennungsdienstliche Behandlung einer Person gemäß § 2 zulässig wäre, die Übermittlung nicht näher determinierter Daten aus dem Ausland. Es wäre klarzustellen, daß als Maximalumfang ebenfalls nur jene Daten übermittelt werden dürfen, die gemäß § 1 Abs. 2 zulässigerweise auch im Inland ermittelt werden dürften.

Zu § 4 Abs. 2: Diese Bestimmung läßt zu, daß eine Sicherheitsbehörde Daten in ihre Verfügungsgewalt nimmt, auch wenn die Voraussetzungen für die erkennungsdienstliche Behandlung des Betroffenen noch nicht vorliegen, da diese Voraussetzungen erst für die Verarbeitung, Benützung, Übermittlung und Überlassung verlangt werden. Da die Zulässigkeit bereits im Ermittlungszeitpunkt gegeben sein muß, erscheint die Bestimmung verfassungsrechtlich bedenklich.

Zu § 6 Abs. 2: Diese Bestimmung sieht vor, daß mit Zustimmung des Betroffenen zusätzlich zu den Daten eines erkennungsdienstlich Behandelten auch Daten jener Personen ermittelt und benützt werden dürfen, die mit dieser Person verwechselt werden können. Im Hinblick auf die Sensibilität der Information und die damit verbundene Gefahr erscheint es notwendig, für diese Zustimmung die Schriftform zu verlangen.

Zu § 7 Abs. 1: Unter "Aktualisierung" im Sinne dieser Bestimmung dürfte primär "Richtigstellung" gemeint sein. Es wäre jedenfalls - so wie dies auch in den Erläuterungen ausgedrückt ist - festzuhalten, daß eine Aktualisierung nur dann erfolgen darf, wenn die Behörde im Rahmen der Vollziehung ihrer gesetzlichen Aufgaben Kenntnis von einer Änderung erlangt. Es wäre jedenfalls verfassungsrechtlich bedenklich, bei einer Person, die erkennungsdienstlich behandelt wurde, eine regelmäßige amtswegige Überprüfung des Aktualitätsgrades dieser Daten vorzunehmen.

Zu § 7 Abs. 2: Die Zusammenfassung spezieller Daten zu "Sonderdateien" ist ein Verarbeiten im Sinne des § 7 des Datenschutzgesetzes. Für derartige Auswertungen muß ebenfalls ein öffentliches Interesse im Sinne des § 1 Abs. 2 DSG iVm Art. 8 Abs. 2 EMRK vorliegen. Die Rechtfertigung für diese Zusammenfassung und der Zweck, welchem diese Daten gewidmet sind, wäre im Gesetz selbst auszudrücken.

Zu § 8 Abs. 1: Den Anmerkungen der Erläuterungen, daß aus Gründen der Einheitlichkeit darauf verzichtet wurde, die Übermittlung an eine zentrale erkennungsdienstliche Evidenz im Gesetz zu normieren, kann nicht gefolgt werden. Dem Gebot des § 7 Abs. 1 Z 1 DSG entsprechend, wonach Datenübermittlungen grundsätzlich eine ausdrückliche gesetzliche Ermächtigung erfordern, sowie aus Gründen der Transparenz, erscheint diese Bestimmung mangelhaft. Die Übermittlungsermächtigung einer nur unpräzise determinierten Verordnung des Bundesministers für Inneres vorzubehalten, erscheint auch verfassungsrechtlich

bedenklich, da die Verfassungsbestimmung des § 1 Abs. 2 DSG iVm Art. 8 Abs. 2 EMRK für Eingriffe in das Grundrecht Gesetze im formellen Sinn verlangen (vgl. etwa VfGH, 12.12.1985, G 225-228/1985). Eine derartige ausdrückliche gesetzliche Ermächtigung im Sinne des § 7 Abs. 1 Z 1 DSG hätte die zu übermittelnden Datenarten, die Zwecke der Übermittlung und die Empfänger abschließend zu regeln (vgl. das Rundschreiben des Bundeskanzleramtes-Verfassungsdienst vom 18. März 1985, GZ 810.099/1-V/1a/85).

Zu § 8 Abs. 2: Es erscheint bedenklich, wenn - wie in den Erläuterungen ausgeführt - die übermittelnde Behörde die Daten ohne Überprüfung weitergeben soll. Es wäre daher in dieser Bestimmung festzuhalten, daß eine Übermittlung nur zulässig ist, wenn ein begründetes Verlangen der ersuchenden Behörde vorliegt, in welchem dargelegt wird, inwieweit die Daten für die Aufgabenerfüllung eine wesentliche Voraussetzung sind. Weiters erscheint es inkonsistent und bedenklich, die erkennungsdienstliche Behandlung von Personen, die befürchten, Opfer eines Verbrechens oder Unfalles zu werden, an die Zustimmung dieser Person zu knüpfen, die Übermittlung dieser Daten jedoch ohne Zustimmung zuzulassen.

Zu § 8 Abs. 3: Gemäß § 32 Abs. 2 Z 1 DSG ist die Übermittlung von verarbeiteten Daten in das Ausland auf Grund von Gesetzen nur dann genehmigungsfrei, wenn in diesen Gesetzen die Datenarten und die Empfänger ausdrücklich genannt sind. Durch den Verweis auf die durch erkennungsdienstliche Maßnahmen ermittelten Daten ist zwar ein entsprechender Determinierungsgrad erreicht, aus Gründen der Rechtssicherheit wäre jedoch in dieser Bestimmung der Übermittlungsinhalt nochmals anzugeben. Der Datenschutzrat bezweifelt jedoch, daß die in dieser Bestimmung angezogenen Identifizierungsdaten tatsächlich abschließend den Inhalt der Evidenzen regeln. Den Erläuterungen zu § 7 Abs. 2 und zu § 8 auf Seite 40 ist zu entnehmen, daß eine sogenannte "Täterkartei" angelegt werden soll, nämlich eine Sammlung von Lichtbildern einschlägiger

Täter. Inhalt der Evidenz ist daher offensichtlich auch der Tattypus, dessen der Betroffene verdächtigt wird. Diese Unterteilung könnte zwar etwa dann akzeptiert werden, wenn bei der Suche nach einem Täter eines Einbruchsdiebstahls einem allfälligen Zeugen dadurch nicht auch Lichtbilder von Trickbetrügern oder anderen Tätertypen gezeigt werden, es wäre jedoch unerläßlich, diesen Inhalt aus Gründen der Rechtssicherheit und zum Zweck der zweifelsfreien Erreichung der Genehmigungsfreiheit gemäß § 32 Abs. 2 Z 1 DSG im Gesetz selbst zu verankern. Die Gliederung nach sachlichen Kriterien ließe sich auch aus den Erläuterungen ableiten.

Zu § 8 Abs. 4: Diese Bestimmung knüpft an eine sachlich nicht ausreichend begründete Spezialdatei, im hier vorliegenden Fall einer "Fremdendatei", und ist ohne Lektüre der erläuternden Bemerkungen unverständlich, da der Gesetzestext eine amtswegige Abgleichung dieser Daten mit jenen anderer Sicherheitsbehörden in regelmäßigen Abständen ermöglichen würde. Wenn daher nach Beseitigung der verfassungsrechtlichen Probleme gegen eine derartige Spezialdatei die von den Erläuterungen ausgedrückte Möglichkeit der Korrektur bestehen soll, wäre dies im Gesetz eindeutiger zu formulieren. Eine amtswegige regelmäßige Abgleichung mit allfälligen anderen Identitätsdaten derselben Person wäre jedenfalls auszuschließen.

Zu § 8 Abs. 6 bis 8: Die Veröffentlichung von Daten bzw. Bekanntgabe an Identitätszeugen darf nur die ultima ratio sein. Darauf nimmt auch § 8 Abs. 8, der anordnet, daß die Übermittlung von Daten nach diesen Bestimmungen nur in dem Umfang geschehen darf, als dies zur Erreichung des angestrebten Zieles notwendig ist und zu dem dadurch bewirkten Eingriff in das Privat- und Familienleben des Betroffenen nicht außer Verhältnis steht, nicht ausreichend Bedacht. Es wäre daher - ähnlich wie in § 8 Abs. 6 Z 1a - zu verankern, daß die Veröffentlichung bzw. Übermittlung nur zulässig ist, wenn das Ziel anders nicht ohne unverhältnismäßigen Aufwand geklärt werden kann. Weiters wäre der Begriff der "beträchtlichen Strafe" zu präzisieren.

Zu § 9: Die Daten inländischen Universitäten zur Auswertung bei nicht personenbezogenen wissenschaftlichen Arbeiten zu übermitteln, ist verfassungswidrig. Die Erläuterungen enthalten keinen Grund, der diesen Grundrechtseingriff im Sinne des § 1 Abs. 2 DSG iVm Art. 8 Abs. 2 EMRK rechtfertigen würde. Die ohne weitere Anmerkungen vorgenommene Berufung auf § 13a des Strafregistergesetzes 1968 reicht als Rechtfertigung jedenfalls nicht aus.

Zu § 10 Abs. 1 Z 3: Diese Bestimmung schreibt die Löschung vor, wenn sich der Verdacht, der zur Aufnahme in die erkennungsdienstliche Evidenz geführt hat, als nicht zutreffend herausstellt, es sei denn, eine weitere Aufbewahrung wäre aus Gründen kriminalpolizeilicher Prävention deshalb unerläßlich, weil auf Grund konkreter Umstände zu befürchten ist, der Betroffene werde den Tatbestand strafbarer Handlungen verwirklichen. Die Erläuterungen zu dieser Bestimmung können nicht überzeugen, da zum einen keinerlei Anhaltspunkte dafür genannt sind, woraus eine Rückfallgefährlichkeit ableitbar sein soll, andererseits in allen Fällen, in denen eine Verurteilung unterbleibt, der Täter wegen dieses Deliktes unbescholten ist. Eine Speicherung trotz fehlender Verurteilung in den in den Erläuterungen angeführten Fällen (Fehlen eines Tatbestandsmerkmales, Verjährung, fehlende Schuldfähigkeit des Täters) ist daher bedenklich. Zur "Rückfallgefährlichkeit" vgl. im übrigen die Anmerkungen zu § 2 Abs. 2.

Zu § 11 Abs. 1 und 2: Unklar bleibt, nach welcher Frist eine Löschung der Daten aus der erkennungsdienstlichen Evidenz auf Antrag des Betroffenen vorgesehen sein soll. Die Anordnung, daß die Löschung dann möglich ist, wenn der Verdacht "schließlich nicht bestätigt werden konnte" ist zu unpräzise. Im übrigen gilt das zu § 10 Abs. 1 Z 3 gesagte.

Zu § 12: Die erläuternden Bemerkungen führen zu dieser Bestimmung aus, daß die im Rahmen kriminalpolizeilicher Tätigkeit ermittelten Daten gespeichert werden sollen. Dem

gegenüber geht § 12 Abs. 1 davon aus, daß die gemäß § 2 Abs. 1 und Abs. 3 Z 1 ermittelten Daten evident zu halten sind. Da davon auszugehen ist, daß die im Rahmen kriminalpolizeilicher Tätigkeit ermittelten Daten darüber hinausgehen, wären die Erläuterungen entsprechend anzupassen.

Zu § 13 Abs. 10: Unklar bleibt, bei welcher Behörde ein Antrag auf Löschung gemäß § 11 des Entwurfes einzubringen ist.

Zu § 17: Die erläuternden Bemerkungen enthalten keinen Rechtfertigungsgrund im Sinne des § 1 Abs. 2 iVm Art. 8 Abs. 2 EMRK, warum die verfassungsrechtlich garantierten Rechte des Betroffenen (Auskunft, Richtigstellung und Löschung) auf den polizeilichen Erkennungsdienst nicht anzuwenden sind. Der bloße Verweis auf § 55 Abs. 2 des Datenschutzgesetzes (Strafregistergesetz 1968) reicht nicht aus. Die Bestimmung ist daher verfassungswidrig.

19. April 1990
Für den Datenschutzrat
Der Vorsitzende:
VESELSKY

Für die Richtigkeit
der Ausfertigung:

REPUBLIK ÖSTERREICH
DATENSCHUTZRAT

A-1014 Wien, Ballhausplatz 1
Tel. (0222) 6615/2528, 2525
Fernschreib-Nr. 1370-900

531 15/O

GZ 816.082/3-DSR/90

Dr. WETTER
2544

Regierungsvorlage zum
Sicherheitspolizeigesetz;

Stellungnahme des Datenschutzrates

An das
Bundesministerium für Inneres

Herrengasse 7
1010 W i e n

Der Datenschutzrat hat zu der mit do. Zl. 112 777/32-I/7/90 vom 16. Juli 1990 übermittelten Regierungsvorlage zum Sicherheitspolizeigesetz in seiner Sitzung am 25. September 1990 folgende

S t e l l u n g n a h m e

beschlossen:

Der Datenschutzrat stellt mit Befriedigung fest, daß eine Reihe seiner Anregungen in den Entwurf eingearbeitet wurden. Soferne Anregungen des Datenschutzrates in der Regierungsvorlage nicht berücksichtigt wurden, wird die mit ho. Schreiben vom 19. April abgegebene Stellungnahme aufrecht gehalten.

Zu § 43:

Der Datenschutzrat geht davon aus, daß § 14 Datenschutzgesetz neben der Sonderbestimmung des § 43 Sicherheitspolizeigesetz zur Anwendung gelangen soll. Diese Auffassung deckt sich auch mit den Ausführungen in den Erläuternden Bemerkungen zu dieser Bestimmung. Im übrigen wird auch hiezu auf die bereits abgegebene Stellungnahme zu § 40 a des Erstentwurfes verwiesen.

Zu den Bestimmungen betreffend eine Geisteskrankenevidenz, eine Umweltevidenz und die Ermittlung und Verarbeitung von Daten zur Vorbeugung rechtswidriger Angriffe erhebt der Datenschutzrat mit Mehrheitsbeschluß (2 Gegenstimmen) keine Einwendungen.

Gegen die Einführung dieser Vorschriften stimmt Univ.Doz. Dr. KOLM mit folgender Begründung:

> "Ich lehne die Stellungnahme des Datenschutzrates ab, weil im Entwurf des Sicherheitspolizeigesetzes Datenermittlung und -verarbeitung insbesondere in Hinblick auf den Begriff der "Vorbeugung" zu weitgehend geregelt sind. Die Führung einer Evidenz über psychisch Kranke ist generell abzulehnen."

Hon.Prof. Dr. DUSCHANEK gibt folgendes Minderheitsvotum ab:

> "Der Begriff "Vorbeugung" als Grundlage der Datenermittlung und -verarbeitung ist im Sinne der Anforderungen des § 1 Abs. 2 DSG zu präzisieren, andernfalls wäre Verfassungswidrigkeit anzunehmen. Der Verweis auf den allgemeinen, ohnehin geltenden Grundsatz der "Verhältnismäßigkeit" ist nicht ausreichend.
>
> Die "Umweltevidenz" (§ 40) ist umweltpolitisch nicht sinnvoll, weil sie den Erfordernissen der Bekämpfung von Umweltkriminalität inhaltlich nicht gerecht wird. Jedenfalls wäre jedoch der Anwendungsbereich auf gefahrengeneigte Anlagen bzw. Störfälle im Sinne der Einheit der Rechtsordnung nach den entsprechenden Definitionen anderer Gesetze (§ 82 a GewO) festzulegen. Zumindest aber hätte die Verordnung gemäß § 40 Abs. 3 des Entwurfes durch Aufzählung der betreffenden Anlagetypen klarzustellen, über welche Anlagen in der Umweltevidenz Daten zu sammeln sind."

25 Ausfertigungen dieser Stellungnahme werden in einem dem Präsidium des Nationalrates übermittelt.

2. Oktober 1990
Für den Datenschutzrat
Der Vorsitzende:
i.A. DOHR

Für die Richtigkeit
der Ausfertigung: