



REPUBLIK ÖSTERREICH
D A T E N S C H U T Z R A T

A-1010 Wien, Ballhausplatz 1
Tel. ++43-1-531 15/0
Fax: ++43-1-531 15/2690
e-mail: dsrpost@bka.gv.at
DVR: 0000019

GZ 817.265/0002-DSR/2004

An das
Präsidium des Nationalrates
Parlament

Dr. Karl Renner Ring 3
1017 Wien

Betrifft: Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz, das Bundesgesetz über die Führung der Bundesgendarmerie im Bereich der Länder und die Verfügung über die Wachkörper der Bundespolizei und der Bundesgendarmerie und das Behörden-Überleitungsgesetz geändert sowie das Gendarmeriegesetz 1894 und das Gendarmeriegesetz 1918 außer Kraft gesetzt werden (SPG-Novelle 2004)-Begutachtungsentwurf des Bundesministeriums für Inneres vom 29. März 2004
Stellungnahme des Datenschutzrates

In der Anlage werden 25 Kopien der Stellungnahme des Datenschutzrates, sowie das im Datenschutzrat abgegebene Votum separatum des Vertreters der Grünen Alternative zu dem im Betreff genannten Gesetzesentwurf übermittelt.

Beilage

15. April 2004
Für den Datenschutzrat
Der stellvertretende Vorsitzende:
WÖGERBAUER



REPUBLIK ÖSTERREICH
D A T E N S C H U T Z R A T

A-1010 Wien, Ballhausplatz 1
Tel. ++43-1-531 15/0
Fax: ++43-1-531 15/2690
e-mail: dsrpost@bka.gv.at
DVR: 0000019

GZ 817.265/0002-DSR/2004

An das
Bundesministerium für Inneres

e-mail: bmi-III-1@bmi.gv.at

Betrifft: Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz, das Bundesgesetz über die Führung der Bundesgendarmerie im Bereich der Länder und die Verfügung über die Wachkörper der Bundespolizei und der Bundesgendarmerie und das Behörden-Überleitungsgesetz geändert sowie das Gendarmeriegesetz 1894 und das Gendarmeriegesetz 1918 außer Kraft gesetzt werden (SPG-Novelle 2004)-
Begutachtungsentwurf des Bundesministeriums für Inneres vom 29. März 2004
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 169. Sitzung am 2. April 2004 beschlossen, zu dem im Betreff genannten Gesetzesentwurf folgende Stellungnahme abzugeben:

§ 13 Abs. 2 SPG:

Dieser Absatz enthält die Ermächtigung zur automationsunterstützten Datenverarbeitung für Zwecke der Dokumentation von Amtshandlungen und der Verwaltung von Dienststücken durch die bezeichneten Sicherheitsbehörden und Polizeikommanden.

Nach der Verfassungsbestimmung des § 1 Abs. 1 DSG 2000 hat jedermann, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

Gemäß Abs. 2 leg. cit. sind, soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Nach der bisherigen Rechtsprechung der Datenschutzkommission müsste es den Sicherheitsbehörden und Wachkörpern - ebenso wie jeder anderen Behörde - selbst ohne ausdrückliche gesetzliche Ermächtigung zugestanden werden, ihr behördliches Handeln zu dokumentieren und die dieser Dokumentation dienenden Akten(-stücke) zu systematisieren, also ein Aktenverwaltungssystem zu führen, weil insoweit ein überwiegendes berechtigtes Interesse an der Datenverarbeitung anzunehmen ist. Nunmehr werden - im Gegensatz zur Vorgängerregelung - die im Rahmen der Aktenverwaltung verarbeitbaren Datenarten demonstrativ aufgezählt, wobei die Notwendigkeit in den erläuternden Bemerkungen mit dem Hinweis auf die Vielschichtigkeit polizeilichen Handelns dargelegt wird. Gleichzeitig wird dort auch klar gestellt, dass es sich nur um ein „Nebenprodukt“ der durch Gesetz festgelegten Aufgaben von Sicherheitsbehörden und Wachkörpern handelt.

Dennoch ist die Gefahr, dass ein derartiges Aktenverwaltungssystem zur Erstellung eines „Personenprofils“ verwendet und damit für einen anderen Zweck missbraucht wird, gerade im Bereich der Sicherheitsverwaltung nicht zu unterschätzen. Diesen Bedenken begegnet der Entwurf, indem eine Abfrage nur nach dem Namen eines Betroffenen bzw. sensiblen Daten nicht möglich ist sondern immer noch ein weiteres Datum angegeben werden muss. Die erläuternden Bemerkungen lassen erkennen, dass besonders die „Ablagevermerke“ eine Abgrenzung nach Sachbereichen ermöglichen und damit als weiteres Datum für die Eingrenzung der Abfrage geeignet erscheinen. Der einen Akt suchende Bedienstete wird in der Regel wissen, welchem Sachgebiet dieser zuzuordnen ist und daher den Ablagevermerk kennen. Ebenso geeignet scheinen andere sachverhaltsbezogene Daten, zB das Datum des protokollierten Vorgangs. In einer derartigen Regelung wäre an sich eine „angemessene Garantie“ zu sehen, sodass der Eingriff in das Grundrecht auf Datenschutz, zu dem § 13 Abs. 2 SPG ermächtigt durch den Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 an sich gedeckt scheint.

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

Es sollte jedoch auch im Gesetzestext noch deutlich zum Ausdruck gebracht werden, dass das für die Abfrage verwendete weitere Datum nicht ein beliebiges sein kann, sondern es sich um ein solches handeln muss, welches den im Rahmen der Aktenverwaltung relevanten Sachverhalt eingrenzt. Daten, die erst recht wieder die Erstellung eines Personenprofils möglich machen (zB bloß das Geschlecht oder auch das Geburtsdatum), scheinen hierfür ungeeignet. Dem Abs. 2 sollte also noch der folgende Halbsatz angefügt werden:

„; vielmehr ist für die Auswahl ein auf den protokollierten Sachverhalt bezogenes weiteres Datum anzugeben.“

§ 35 Abs. 1 Z 8 SPG

Diese Bestimmung ermächtigt zu einer Identitätsfeststellung durch die Organe des öffentlichen Sicherheitsdienstes, wenn dies zum Zwecke der Feststellung, ob sich der Betroffene an einer Örtlichkeit aufhält, an der für ihn ein Betretungsverbot besteht, notwendig ist.

Die Feststellung der Identität stellt ohne Zweifel eine Ermittlung personenbezogener Daten und damit einen Eingriff in das Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 dar. An sich wird man ein überwiegendes berechtigtes Interesse an einer Feststellung, ob sich jemand unrechtmäßig an einem Ort aufhält, nicht verneinen können, weil sonst die Effektivität jedes individuellen Betretungsverbots (zB bei Gewalt in Wohnungen nach § 38a SPG) in Frage stünde.

Die vorliegende Ermächtigung ist jedoch insofern zu weit reichend, als – anders als in sämtlichen anderen Tatbeständen des § 35 Abs. 1 SPG – nicht auf „bestimmte Tatsachen“ bzw. zumindest die „Umstände“ der jeweiligen Situation abgestellt wird, sondern eine Identitätsfeststellung bei faktisch jedermann zulässt.

§ 35 Abs. 1 Z 8 sollte daher folgendermaßen umformuliert werden:

„8. wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sich der Betroffene an einer Örtlichkeit aufhält, an der für ihn ein Betretungsverbot besteht.“

Die Einschränkung auf das Vorliegen „bestimmter Tatsachen“ wahrt die Verhältnismäßigkeit des Eingriffs, sodass diesfalls tatsächlich von einem überwiegenden berechtigten Interesse auszugehen ist.

§ 36a Schutzzone

Der Datenschutzrat verweist im Hinblick auf Art. 2 des 4. Zusatzprotokolls zur Europäischen Menschenrechtskonvention BGBl 1969/434 idF BGBl III 1998/30, das generell bei Eingriffen

in Grundrechte immer der Grundsatz der Verhältnismäßigkeit zu berücksichtigen ist und es im gegebenen Fall zu keiner extensiven Ausdehnung von Schutzzonen in Österreich kommen sollte.

§ 53 Abs. 1 Z 2a SPG:

Der nunmehrige Inhalt dieser Bestimmung ist auch unter Heranziehung der Erläuterungen nicht erschließbar. Der Zweck der Verarbeitung personenbezogener Daten kann nicht im „Einsatz von Bild- und Tonaufzeichnungsgeräten an öffentlichen Orten“ liegen, weil es sich dabei nur um das eingesetzte Mittel zur Datenermittlung handelt. Auch der Hinweis auf § 54 Abs. 6 SPG (s. sogleich unten) führt nicht zu besserem Verständnis, weil gerade diese Bestimmung eine Löschung von durch Bild- und Tonaufzeichnung gewonnenen Daten nach 48 Stunden vorsieht und damit bereits von einer Datenermittlung – auch diese stellt gemäß § 4 Z 9 DSG 2000 bereits eine Verarbeitung der Daten dar – ausgeht.

Sollte gemeint sein, dass eine *Weiterverarbeitung* (zB elektronische Auswertung) erst nach drei Tagen erfolgen soll, wäre diese hinreichend zum Ausdruck zu bringen. Völlig unklar ist auch der Beginn der dreitägigen Frist. Eine detaillierte Neuformulierung dieser Bestimmung wäre daher anzuraten.

§ 54 Abs. 6 SPG¹

Diese Bestimmung ermächtigt die Sicherheitsbehörden zum „Ermitteln personenbezogener Daten Anwesender mit Bild- und Tonaufzeichnungsgeräten“ an „öffentlichen Orten“, also zu sogenannter Video- /Audioüberwachung, wenn auf Grund bestimmter Tatsachen, insbesondere wegen vorangegangener gefährlicher Angriffe, zu befürchten ist, dass es an öffentlichen Orten zu gefährlichen Angriffen gegen Leben, Gesundheit oder Eigentum von Menschen kommen wird. Als Zweck der Ermittlung wird die „Vorbeugung solcher Angriffe“ angeführt, die ermittelten Daten dürfen aber auch zur Abwehr und Aufklärung gefährlicher Angriffe sowie für Zwecke der Fahndung verwendet werden.

Es ist zunächst festzustellen, dass insbesondere die Videoüberwachung zumindest hinsichtlich gewisser aufgezeichneter Personen ein Ermitteln personenbezogener Daten darstellt und damit in das Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 - darüber

¹ Die Ausführungen zu dieser und der folgenden Bestimmung beruhen zum Teil auf der Stellungnahme der gemäß Art. 29 der Datenschutzrichtlinie eingerichteten Gruppe vom 11. Februar 2004 zum Thema „Processing of Personal Data by means of Video Surveillance“, die sich hauptsächlich mit der Zulässigkeit von Videoüberwachung im Anwendungsbereich der Datenschutzrichtlinie befasst. Ob sich dieser auch auf sicherheitspolizeiliche Tätigkeiten erstreckt, könnte besonders im Lichte jüngster (Österreich betreffender) EuGH-Rechtsprechung fraglich sein. Dennoch scheinen die Ausführungen in der Stellungnahme zum Großteil auch für die österreichische Rechtslage brauchbar, weil das DSG 2000 die in der Richtlinie verankerten Grundsätze größtenteils auch auf nicht von der „ersten Säule“ umfasste Bereiche ausdehnt.

hinaus wohl auch in die Rechte auf ein Privat- und Familienleben (Art. 8 EMRK) und Freizügigkeit der Person (Art. 2 4. ZPEMRK) - eingreift. Es ist weiters nicht ausgeschlossen, dass auch sensible Daten (§ 4 Z 2 DSG 2000) ermittelt werden können und es ist ausdrücklich genanntes Ziel der Regelung, Daten zumindest über gerichtlich strafbare Handlungen von Personen zu gewinnen, um diese dann auch zur Strafverfolgung einsetzen zu können. Dies ergibt sich rechtlich aus der Definition des „gefährlichen Angriffs“ in § 16 SPG. Damit liegen jedenfalls Daten vor, die im Sinn des § 1 Abs. 2 DSG 2000 ihrer Art nach besonders schutzwürdig sind und deren Ermittlung jedenfalls „angemessene Garantien“ erforderlich machen.

Gemäß § 1 Abs. 2 DSG 2000 ist zu prüfen, ob ein das Geheimhaltungsinteresse des Einzelnen überwiegendes berechtigtes Interesse der Sicherheitsbehörden an der Ermittlung seiner personenbezogenen Daten vorliegt und die Maßnahme aus einem der in Art. 8 Abs. 2 EMRK genannten Gründe notwendig ist. Dabei ist insbesondere zu berücksichtigen, dass die Geheimhaltungsinteressen einzelner Personen hinsichtlich ihres Verhaltens an öffentlich zugänglichen Orten eindeutig geringer anzusetzen sind als etwa in privaten, nicht jedermann zugänglichen Räumlichkeiten, insbesondere Wohnungen, weil an öffentlichen Orten stets mit einer Beobachtung durch andere Personen zu rechnen ist. Dies ist bei Anwendung der vorliegenden Bestimmung umso mehr anzunehmen, als eine weit reichende Ankündigungspflicht der Sicherheitsbehörden besteht. Der Eingriff ist auch deshalb verhältnismäßig geringfügig, weil es zu einer weiteren Verarbeitung der ermittelten Daten nicht kommen darf, wenn nicht die Abwehr bzw. Verfolgung gerichtlich strafbarer Handlungen dies erforderlich machen. Diese Argumente sprechen dafür, ein überwiegendes berechtigtes Interesse der Sicherheitsbehörden grundsätzlich anzunehmen.

Die Maßnahme dient auch den in Art. 8 Abs. 2 EMRK genannten Zielen der Verhinderung von strafbaren Handlungen sowie dem Schutz der Rechte und Freiheiten anderer, nämlich der von gerichtlich strafbaren Handlungen (gefährlichen Angriffen) bedrohten Personen. Die Ankündigungspflicht, das ausdrückliche Lösungsgebot nach 48 Stunden sowie die Einbindung des Rechtsschutzbeauftragten (auch wenn dessen Einrichtung nach der jüngsten Rechtsprechung des VfGH bei der derzeitigen Verfassungsrechtsslage als verfassungswidrig anzusehen sein dürfte) stellen angemessene Garantien für den Schutz der ohne Frage nach wie vor bestehenden Geheimhaltungsinteressen der Betroffenen dar.

Der Datenschutzrat regt weiters an, die Rolle des Rechtsschutzbeauftragten im Gesetz noch genauer zu konkretisieren.

Bei Missbrauch besteht gemäß § 1 Abs. 5 DSG 2000 die Möglichkeit einer Beschwerde an die Datenschutzkommission und somit ein angemessener Rechtsschutz.

Es sollten einige Klarstellungen erfolgen:

Beim Begriff des „öffentlichen Ortes“ sollte auf § 27 Abs. 2 SPG verwiesen werden.

Nicht ganz glücklich gewählt scheint der Begriff der „Fahndung“. Dieser wird an sich in § 24 SPG definiert. § 54 Abs. 6 SPG scheint aber nur auf die Verhinderung gefährlicher Angriffe bzw. die Aufklärung von Straftaten gerichtet, nicht aber etwa auf die Feststellung von Selbstmorden bzw. die Suche nach potentiellen Verbrechensopfern (§ 24 Abs. 1 Z 2 SPG). Auch hier sollte zumindest (etwa durch einen Verweis auf § 24 SPG oder die Streichung des Halbsatzes „sowie für Zwecke der Fahndung“) Klarheit geschaffen werden.

- § 12 Abs. 1a GrekoG

Diese Bestimmung ermächtigt zum Einsatz von Bild- und Tonaufzeichnungsgeräten im Rahmen der Grenzkontrolle. Grenzkontrolle ist gemäß § 1 Abs. 2 GrekoG die aus Anlass eines beabsichtigten oder bereits erfolgten Grenzübertritts vorgenommene Überprüfung der Einhaltung der die Sicherheitspolizei, das Passwesen, die Fremdenpolizei sowie der das Waffen-, Schieß- und Sprengmittelwesen regelnden bundesgesetzlichen Vorschriften.

Obwohl die Zwecke der Grenzkontrolle grundsätzlich bereits normiert sind, wäre auch hier anzuraten, eine Neufassung zu formulieren, welche die Zwecke einer Video-/Audioüberwachung noch eindeutiger und detaillierter festlegt, damit eine Prüfung am Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 möglich wird.

Abgesehen von diesem Bedenken ist zu bemerken, dass wie schon zuvor bei § 53 Abs. 1 Z 2a SPG auch hier der Beginn der dreitägigen Frist nicht eindeutig ist. Diesbezüglich sollte jedenfalls eine Klarstellung getroffen werden.

15. April 2004
Für den Datenschutzrat
Der stellvertretende Vorsitzende:
WÖGERBAUER

Votum Separatum zur geplanten Ausweitung der Videoüberwachung durch das Innenministerium (Abgegeben am 2.4.04 von Dr. Hans G. Zeger im Rahmen der Sitzung des Datenschutzrates):

„Entwurf: Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz, das Bundesgesetz über die Führung der Bundesgendarmerie im Bereich der Länder und die Verfügung über die Wachkörper der Bundespolizei und der Bundesgendarmerie und das Behörden-Überleitungsgesetz geändert sowie das Gendarmeriegesetz 1894 und das Gendarmeriegesetz 1918 außer Kraft gesetzt werden (SPG-Novelle 2004),

Zusätzliche Überwachungsmaßnahmen von öffentlich-rechtlichen und privat-rechtlichen Einrichtungen können nur unter dem Gesichtspunkt der Verhältnismäßigkeit der Wirksamkeit der eingesetzten Methoden und Mittel gegenüber den Eingriffen in die Privatsphäre der Betroffenen beurteilt werden. Auch Reisefreiheit, öffentliche Meinungsäußerungen oder das unbeobachtete Treffen mit anderen Personen an bestimmten Orten fallen unter den Privatsphärebegriff und sind durch die Europäische Menschenrechtskonvention besonders geschützt.

Die Steigerung des 'Sicherheitsgefühls' oder andere Plazebomaßnahmen zur Sicherheitspolitik, das Appellieren an niedere Instinkte und das Schüren der Emotionen in der Bevölkerung gegen abweichendes Verhalten und auffällige Personengruppen, können keinesfalls Grundlage der Rechtfertigung von Eingriffen in die Privatsphäre und in die informationelle Selbstbestimmung der Menschen darstellen.

Weltweit gilt das auffällige Beobachten von Menschen als aggressiver Akt und wird in vielen Ländern unter den Begriff 'Stalker' unter Strafdrohung gestellt. Selbst das Innenministerium hat dazu Anfang des Jahres eine Initiative zur Zurückdämmung des unerwünschten Beobachtens durch Dritte gestartet.

Die vorliegenden Überwachungspläne gehen eindeutig in Richtung des auffälligen Beobachtens und fallen daher grundsätzlich unter den 'Stalker'-Begriff. Auch wenn bei bestimmten Fällen geplant ist, die Videoüberwachung anzukündigen und auch wenn davon ausgegangen werden muss, dass das Recht auf Selbstbestimmung im öffentlich zugänglichen Raum geringer ist, als etwa in der eigenen Wohnung, bestehen Grundrechtsinteressen. Selbst wenn nur geringfügige Eingriffe in diese Persönlichkeitsrechte vorliegen, muss die Frage der Verhältnismäßigkeit gestellt werden.

Selbst nach ausführlichen Recherchen und nach intensiver Befragung von 'informierten Vertretern' des Innenministeriums konnten keinerlei Hinweise ermittelt werden, dass die schon jetzt langjährig bestehenden polizeilichen Überwachungslösungen, zur Aufklärung von Verbrechen beitragen. Selbst der Beitrag bei der Aufklärung kleinerer Vergehen ist geringfügig und nicht wesentlich höher als die Aufklärungsquote durch beherzte ältere Damen, die Täter auf frischer Tat stellen. Auch der Beitrag der privaten Videoinstallationen zur Verbrechensaufklärung ist durch das Innenministerium nicht quantifizierbar und offenbar vernachlässigbar gering.

Andere Ziele, wie die Verbrechensvermeidung, Prävention oder Verhinderung von Straftaten werden ganz offensichtlich nicht erreicht, wie die Daten für 2003 zeigen, die mit 654.381 Delikten (+10,6%) besonders ein Ansteigen im Bereich der Kleinkriminalität zeigen.

Auf Grund der enormen Kosten, des hohen Verwaltungs- und Auswertungsaufwandes von Videoinstallationen und der relativen Unbeweglichkeit einer einmal erfolgten Installation, können Videoüberwachungsmaßnahmen sowieso nur extrem punktuell stattfinden. Es muss daher befürchtet werden, dass damit Ressourcen fehlen werden, die flächendeckend für Österreich ein gleichhohes Sicherheitsniveau erreichen. Ein weiteres enormes Ansteigen der (Klein)Kriminalität in den überwachungsfreien Zonen ist damit absehbar.

Die geplanten zusätzlichen Überwachungs- und Aufzeichnungsrechte des Innenministeriums müssen als nicht zweckgerichtet und daher als unverhältnismäßige Eingriffe in das Privatleben der Menschen angesehen werden. Dies gilt besonders unter Bedachtnahme, dass Spanner-Interessen, Voyeurismus und das Beobachten anderer Leute bei vielen Menschen beliebt sind und daher Videoüberwachung populär ist. Es wäre jedoch Aufgabe des Innenministeriums derartigen Emotionen gegenzusteuern und überzeugende flächendeckende Konzepte vorzulegen, die zu einem tatsächlichen Heben des Sicherheitsniveaus führen.“