Nr. 14/01

Thema: Verfahren betreffend Überprüfung gemäss Art. 14 Abs. 3 ZentG

Art. 14 Abs. 3 ZentG. Aufbewahrungsfristen. Telefonüberwachung. Richtigkeit von Personendaten.

- Eine globale Übernahme aus alten Informationssystemen in ein neues Informationssystem muss mit Kontrollen der Richtigkeit, insbesondere der Aktualität und Integrität der Personendaten, und Notwendigkeit im Einzelfall verbunden werden. (E. 1.)

- Bei ungeprüft als gesichert übernommenen Daten ist eine Überprüfung im Einzelfall noch durchzuführen. (E. 2.)

- Informationen aus Telefonüberwachungen dürfen ausserhalb des Strafverfahrens nicht für beliebige kriminalpolizeiliche Zwecke verwendet werden. (E. 3a.)

- Über verdächtige Personen und Unternehmen sollten keine geheim zu haltenden Lage- und Bedrohungsberichte verbreitet werden, wenn die Strafverfolgungsbehörde im Verfahren die Parteirechte der Betroffenen nicht entsprechend Art. 32 BV und Art. 6 EMRK gewährleisten kann. (E. 5.)

- Die Regelung der Aufbewahrungsfristen muss differenzierter ausgestaltet werden. (E. 6.)

Thème: Procédure concernant la vérification selon art. 14 al. 3 LOC

Art. 14 al. 3 LOC. Délais de conservation. Surveillance téléphonique. Exactitude de données personnelles

- Toute reprise globale de données provenant d'anciens systèmes d'information dans un nouveau système d'information doit être liée à des contrôles permettant d'en vérifier l'exactitude, et notamment l'actualité et l'intégrité des données personnelles, ainsi que l'opportunité de la reprise, ceci dans chaque cas particulier. (Consid. 1.)

- Lorsqu'il s'agit de la reprise de données non vérifiées considérées comme assurées, il faut dans chaque cas particulier procéder une nouvelle fois à une vérification. (Consid. 2.)

- En dehors du cadre d'une procédure pénale, les informations provenant de surveillances téléphoniques ne peuvent pas être utilisées à des fins quelconques de police criminelle. (Consid. 3a.)

- Les rapports de situation et de menaces concernant des personnes et des entreprises soupçonnées devant être tenus secrets ne devraient pas être divulgués lorsque les autorités de poursuites pénales ne peuvent assurer les droits des parties des personnes concernées au sens des art. 32 Cst. et art. 6 CEDH pendant la procédure. (Consid. 5.)

- La réglementation concernant les délais de conservation doit être établie de manière plus différenciée. (Consid. 6.)

Entscheid vom 28. September 2006

(Ausfertigung 22. Dezember 2006)

Mitwirkend: Prof. Dr. R.J. Schweizer (Präsident), Frau T. Mona (Instruktionsrichterin), Frau Fürsprecherin Dr. U. Widmer sowie Fürsprecher M. Sterchi (Sekretär)

Im Verfahren betr. Überprüfung gemäss Art. 14 Abs. 3 ZentG in Sachen

A., vertreten durch RA X.

Gesuchsteller

gegen

1. **Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten,** Feldeggweg 1, 3003 Bern,
2. **Bundesamt für Polizei (BAP), nun fedpol**, 3003 Bern.

wird festgestellt:

A. Mit Schreiben vom 30. Mai 2001 [Datumsangaben im ganzen Entscheid geändert] machte der Gesuchsteller das Auskunftsrecht nach Art. 14 Abs. 2 des Bundesgesetzes vom 7. Oktober 1994 über kriminalpolizeiliche Zentralstellen des Bundes (ZentG; SR 360) geltend. Der Eidgenössische Datenschutzbeauftragte (EDSB; heute: Eidg. Datenschutz- und Öffentlichkeitsbeauftragter, EDÖB) teilte ihm am 28. August 2001 in der stets gleichlautenden Mitteilung nach Art. 14 Abs. 2 ZentG mit, dass in Bezug auf ihn entweder keine Daten unrechtmässig bearbeitet werden, oder dass der EDSB bei Vorhandensein allfälliger Fehler in der Datenbearbeitung eine Empfehlung zu deren Behebung an das Bundesamt für Polizei (BAP) gerichtet habe. Mit Schreiben vom 24. November 2001 ersuchte der Gesuchsteller die Eidgenössische Datenschutzkommission (EDSK; heute: Eidg. Datenschutz- und Öffentlichkeitskommission, EDÖK) um Überprüfung der Mitteilung des EDSB.

B. Am 3. Dezember 2001 führte die damalige Instruktionsrichterin, Frau Fürsprecherin A. Stegmann, und der Sekretär der EDSK, Herr Fürsprecher M. Sterchi, einen Augenschein bei der Bundeskriminalpolizei durch. Dabei stellten sie fest, dass der Gesuchsteller seit dem 1. April 1996 im JANUS bzw. in entsprechenden Vorgängersystemen als sog. Stammperson registriert ist. Unter diesem Stamm waren insgesamt 32 Vorgänge registriert, welche sich auf fünf verschiedene Dossiers bezogen. Hingegen war der Gesuchsteller im System der Meldestelle für Geldwäscherei GEWA nicht verzeichnet.

Im Subsystem "Journal" fanden sich drei Einträge im Zusammenhang mit einer bestimmten Polizeiaktion aus dem Jahre 1998.

In der Geschäftskontrolle fanden sich 25 Einträge, die sich auf zwei verschiedene Dossiers bezogen.

Das Ergebnis der Kontrolle stimmte mit der Überprüfung durch den EDSB überein.

C. In Zusammenhang mit der Überprüfung des Auskunftsersuchens des Gesuchstellers erliess der EDSB am 11. September 2001 eine einlässlich begründete Empfehlung. Darin wurde gefordert, dass:

1. die Bundeskriminalpolizei sicherstellt, dass zuhanden der Sachbearbeiter, die bei den indirekten Auskunftsgesuchen für die Suche im Datenverarbeitungssystem JANUS zuständig sind, eine spezifische automatisierte "Abfrageroutine" so rasch als möglich ausgearbeitet wird, die die verschiedenen Etappen und die verschiedenen Abfragekriterien enthalten, die nötig sind, damit gewährleistet ist, dass eine Person tatsächlich eingetragen resp. nicht eingetragen ist;
2. die Bundeskriminalpolizei dafür sorgt, dass inskünftig bei der Überprüfung von indirekten Auskunftsgesuchen gemäss Art. 14 ZentG mit absoluter Sicherheit garantiert werden kann, dass Personen, bei denen die Suche im System JANUS keinen Eintrag ergeben, tatsächlich nicht in der Datenbank JANUS eingetragen sind und auch keine Unterlagen in Papierform vorhanden sind. Desgleichen, dass Gewähr dafür besteht, dass in denjenigen Fällen, in denen Einträge im System gefunden wurden, tatsächlich keine weiteren Einträge oder Unterlagen vorhanden sind. Und schliesslich, dass sämtliche, im elektronischen System JANUS vorhandenen Einträge beim Bundesamt für Polizei (BAP; heute: Fedpol) selbst auch in Papierform vorliegen;
3. angesichts der Tatsache, dass – wie dies aus dem Vorerwähnten ersichtlich ist – das indirekte Auskunftsrecht nicht gesetzeskonform ausgeübt und die Richtigkeit der durch die Bundeskriminalpolizei bearbeiteten Daten nicht gewährleistet werden kann, das BAP zuhanden des EDSB einen ausführlichen Kalender betreffend die zeitliche Realisierung der vom BAP vorgesehenen Massnahmen erstellt;

4. die Bundeskriminalpolizei den EDSB benachrichtigt, sobald die verlangten Massnahmen ergriffen wurden, damit weitere, zukünftige Auskunftsgesuche wie gesetzlich vorgesehen, erledigt werden können.

Der EDSB verlangte vom BAP, dass es ihm mitteilt, ob es bzw. die Bundeskriminalpolizei die Empfehlung annehme, und verwies auf die Kompetenz des EDSB, die Empfehlung bei Ablehnung oder Nichtbefolgung dem EJPD zu unterbreiten.

Das BAP teilte dem EDSB mit Schreiben vom 26. September 2001 mit, dass man sich der Problemlage bewusst sei, dass aber die Forderungen des EDSB in dieser Absolutheit nicht erfüllbar seien, weil es an der praktischen Durchführbarkeit mangle. Verbesserungen seien im Gange, benötigten aber mehr Zeit. Aus diesen Gründen lehnte das BAP die Empfehlung ab.

Andere Empfehlungen erliess der EDSB in Zusammenhang mit der Überprüfung des Auskunftsersuchens des Gesuchstellers nicht.

D. Am 29. August 2003 führte die EDSK unter dem Vorsitz des Präsidenten eine Instruktionsverhandlung durch. Anschliessend wurde die Instruktion schriftlich fortgesetzt. Das BAP reichte am 30. Januar 2004 einen schriftlichen Bericht ein.

Die Eidgenössische Datenschutz- und Öffentlichkeitskommission zieht in Erwägung:

1. a) Rechtsfragen ergaben sich durch die Art und Weise der Übertragung von Personendaten aus dem Zentralen Aktennachweis (ZAN) an ISOK und DOSIS resp. heute JANUS. Aus den Ausführungen des BAP an der Instruktionsverhandlung vom 29. August 2003 ergibt sich, dass die Daten aus ZAN elektronisch in die anderen Systeme übertragen wurden. Nach Art. 11 Abs. 3, zweiter Satz ZentG ist das Informationssystem JANUS der Zentralstellen von anderen Informationssystemen der Polizei und der Verwaltung getrennt zu führen. Eine elektronische Schnittstelle zwischen ZAN einerseits und JANUS verletzt diese Vorschrift.

b) Das ZentG enthält nur wenige materielle Datenschutzvorschriften. Die Botschaft begründete dies damit, dass die weiteren Regelungen technischer Natur seien und deshalb nicht in ein Gesetz, sondern in eine Verordnung gehörten. Deshalb enthalte das Gesetz (heute in Art. 11 ZentG) nur "rechtsstaatlich notwendige Eckpfeiler für datenschutzrechtliche Grundsätze" (BBl 1994 I 1162). Bei Art. 11 Abs. 3, zweiter Satz ZentG handelt es sich somit nicht bloss um eine reine Ordnungsvorschrift, sondern – jedenfalls nach Ansicht des Gesetzgebers – um einen Eckpfeiler rechtsstaatlicher Datenbearbeitung. Auch wenn nachvollziehbar ist, dass die Übertragung grosser Datenmengen aus Gründen der Effizienz elektronisch und nicht manuell erfolgen soll, so verlangt das verfassungs-

rechtliche Trennungsgebot von präventiver Informationsbearbeitung vor gerichtspolizeilichen Ermittlungsverfahren und der Datenbearbeitung in gerichtspolizeilichen Verfahren eine **einzelfallweise Überprüfung der Richtigkeit und Notwendigkeit der zu übernehmenden Daten.** Andernfalls müsste zumindest das ZentG angepasst werden.

2. a) Aus dem erwähnten Bericht des BAP/fedpol vom 30.1.2004 ergibt sich, dass die aus dem ZAN übernommenen Daten nie als gesichert oder ungesichert qualifiziert wurden (S. 3 des Berichtes). Als Grund gibt das BAP an, dass diese Qualifizierung der Daten im ZAN nicht existiert habe. Die Beurteilung der Daten aus ZAN im Hinblick auf ihre Zuverlässigkeit habe anlässlich der Übertragung der Daten in ISOK wegen der grossen Datenmenge nicht durchgeführt werden können. Man habe alle Daten bei der Übertragung aus ZAN als gesichert qualifiziert, weil die Aufbewahrungsdauer für ungesicherte Daten nach der ISOK-Verordnung (Art. 15) nur zwei Jahre betragen hätte. Man habe nicht alle Daten aus ZAN schon nach 2 Jahren verlieren, sondern von der 10-jährigen Aufbewahrungsfrist für gesicherte Daten profitieren wollen.

   b) Diese Praxis des BAP verstösst zunächst gegen den heute aufgehobenen Art. 10 Abs. 1 der ISOK-Verordnung. Gemäss dieser Bestimmung mussten die Daten bei der Eingabe als gesichert oder ungesichert qualifiziert werden, und zwar anhand ihrer Herkunft, der Art der Übermittlung, ihres Inhaltes und bereits vorhandener Daten. Nach Art. 10 Abs. 4 der ISOK-Verordnung hätte der Kontrolldienst die Qualifizierung nach Eingabe der Daten überprüfen müssen. Die gleiche Regelung wurde auch in den Nachfolgeverordnungen übernommen. Im geltenden Recht enthalten Art. 12, 12a und 13 der Verordnung vom 30. November 2001 über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung; SR 360.2) eine ähnliche Regelung. Ferner verpflichtet namentlich Art. 14 Abs. 2 Bst. a der JANUS-Verordnung den Kontrolldienst im Rahmen der periodischen Gesamtüberprüfung auch, die Qualifizierung der Daten hinsichtlich ihrer Zuverlässigkeit zu überprüfen.

   c) **Die Qualifizierung der Daten muss in jedem Einzelfall vorgenommen werden.** Wenn die Qualifizierung bei der "Migration" der Daten nicht vorgenommen wurde, so hätte sie somit spätestens bei der nachfolgenden periodischen Gesamtüberprüfung vorgenommen werden müssen. Jedenfalls enthielt weder die ISOK-Verordnung (oder eine der anderen zwischenzeitlich aufgehobenen Ausführungsverordnungen zum ZentG), noch enthält das heute geltende Recht (JANUS-Verordnung vom 30. November 2001) eine entsprechende Ausnahme von der Prüfung der Qualifizierung von Daten als gesichert bzw. ungesichert.

3. Eine kritische Frage stellt sich hinsichtlich der **Verwendung von Informationen aus Telefonüberwachungen.**

a) Im vorliegenden Verfahren hat die Kommission festgestellt, dass Daten, die aus einer Telefonüberwachung eines unbekannten Dritten stammen, aber Aussagen über den Gesuchsteller beinhalten, in dessen Datensätzen auftauchen bzw. weiterbearbeitet werden. Das BAP führt in seinem Bericht vom 30. Januar 2004 aus (S. 11 Mitte): "Die zuständigen Behörden können aber Informationen aus gerichtspolizeilichen Verfahren aus Telefonkontrollen im JANUS zu den Stammdaten erfassen."

   Dies ist so generell unzutreffend. Nach geltendem Recht (Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs; BÜPF; SR 780.1) dürfen Daten aus der Überwachung des Post- und Fernmeldeverkehrs für das Strafverfahren verwendet werden, in welchem sie erhoben wurden (Art. 8); nicht mehr notwendige Informationen sind auszuscheiden. Ferner besteht ausnahmsweise und in gewissen Grenzen die Möglichkeit der Verwertung von Zufallsfunden (Art. 9). Stets vorausgesetzt wird, dass die Überwachungsmassnahmen **Erkenntnisse über (weitere) Straftaten** liefern. Irgendwelche Informationen, die keinen Hinweis auf begangene Straftaten liefern, dürfen nicht verwendet werden. Ferner sieht das BÜPF nur die **Verwendung** von Informationen aus der Überwachung des Post- und Fernmeldeverkehrs **in Strafverfahren** vor. Ausserhalb von Strafverfahren dürfen solche Informationen nicht verwendet werden. Dann unterscheidet Art. 9 BÜPF zwischen der genehmigungsfreien Verwendung von Informationen und der Verwendung von Informationen, die der Zustimmung der Genehmigungsbehörde bedürfen. Werden andere als die in der Überwachungsanordnung aufgeführten Straftaten bekannt, so dürfen diese Erkenntnisse unter gewissen Voraussetzungen gegen die (in der Überwachungsanordnung) verdächtigte Person ohne Genehmigung verwendet werden (Art. 9 Abs. 1). Betreffen die Erkenntnisse Straftaten einer Person, die in der Anordnung keiner Straftat verdächtigt wird, muss vor Einleitung weiterer Ermittlungen die Zustimmung der Genehmigungsbehörde eingeholt werden. (Art. 9 Abs. 2).

b) In Hinblick auf das geltende Recht ist die Praxis des BAP aus verschiedenen Gründen problematisch.

   Zum Ersten ist im BÜPF nur die Verwendung von Informationen aus der Überwachung des Post- und Fernmeldeverkehrs **für die Durchführung von Strafverfahren** vorgesehen. JANUS dient aber nicht nur der Durchführung von Strafverfahren. Die vielfältigen kriminalpolizeilichen Zwecke, denen JANUS dient, lassen sich einmal aus Art. 2 der JANUS-Verordnung entnehmen. Ferner ist aus Art. 3 der JANUS-Verordnung ersichtlich, dass das System auch rein präventiven Zwecken dient. Die Informationen aus JANUS können zudem für vielfältigste Aufgaben auch ausserhalb von Strafverfahren bekannt gegeben werden (vgl. dazu Art. 16 f. der JANUS-Verordnung). Werden Informationen aus der Überwachung des Post- und Fernmeldeverkehrs den Stammdaten zugeführt, stehen sie allen diesen Verwendungszwecke offen. Offensichtlich wird für die Speicherung solcher Informationen unter den Stammdaten nicht die Zustimmung der

Genehmigungsbehörde eingeholt; denn diese dürfte ihre Zustimmung zu einer solchen Verwendung gar nicht erteilen. Die aus Telefonüberwachungen gewonnenen Informationen werden auch nicht mit einer Verwendungsbeschränkung versehen.

Zum Zweiten müsste es sich um so genannte Zufallsfunde handeln (Art. 9 BÜPF). Ein Zufallsfund liegt vor, wenn durch eine Überwachung **andere strafbare Handlungen** bekannt werden. Das Besorgen eines Anwaltes ist keine strafbare Handlung (vgl. den Bericht fedpol vom 30. Januar 2004, S. 8 betr. DosCH 231020 NR). Somit kann sachlich kein relevanter Zufallsfund vorliegen.

Schon vor Inkrafttreten des BÜPF galt in Verfahren nach BStP eine ähnliche Regelung: Nach Art. 66 Abs. 1ter BStP waren Aufzeichnungen, die für die Untersuchung nicht notwendig sind, gesondert unter Verschluss zu halten und nach Abschluss des Verfahrens zu vernichten. Eine Verwendung von Informationen aus der Überwachung des Post- und Fernmeldeverkehrs ausserhalb des Verfahrens, in welchem die Massnahme angeordnet worden war, war im BStP überhaupt nicht vorgesehen (vgl. dazu auch JUDITH NATTERER, Die Verwertbarkeit von Zufallsfunden aus Telefonüberwachung im Strafverfahren, Bern 2001, S. 34 ff., insb. Fn. 122).

Das BAP führte in seinem Bericht vom 30.1.2004 (S. 11) aus, dass die Information, wonach der Gesuchsteller jemandem einen Anwalt besorgen sollte, aus einer Telefonabhörung stammt, die in einem Verfahren unter Leitung des Bundesanwaltes erfolgt war. Somit hätte die Regelung von Art. 66 Abs. 1ter BStP angewendet werden müssen. Die Information hätte nicht in ISOK bzw. JANUS unter dem Stamm des Gesuchstellers gespeichert werden dürfen.

c) Das BAP stellt sich auf den Standpunkt, dass Telefonkontrollen bzw. Überwachungen des Post- und Fernmeldeverkehrs nur im Rahmen von Strafverfahren stattfinden dürfen, deshalb falle dieser Bereich nicht unter das Datenschutzgesetz (Art. 2 Abs. 2 lit. c DSG) und unterliege nicht der Prüfung durch die EDSK (vgl. Bericht des BAP vom 30.1.2004, S. 11). Die Auffassung ist unter verschiedenen rechtlichen Gesichtspunkten unzutreffend:

Zum Einen handelt es sich im vorliegenden Fall gerade nicht um die Verwendung von Informationen in Strafverfahren, sondern um die Verwendung von Informationen aus der Überwachung des Post- und Fernmeldeverkehrs ausserhalb von Strafverfahren. Konkret handelt es sich um eine nach dem BÜPF verbotene Verwendung. Die Daten über den Gesuchsteller wurden in ISOK bzw. JANUS gespeichert und werden heute (d.h. zum Zeitpunkt der vorgenommenen Kontrolle) in JANUS bearbeitet. Ob nun durch die Bearbeitung dieser Daten in JANUS der BStP oder das BÜPF verletzt werden oder nicht, handelt es sich in jedem Fall um eine ein hängiges Strafverfahren überschreitende Bearbeitung von Personendaten in den Zentralstellen bzw. bei der Bundeskriminalpolizei. Nach Art. 14 Abs. 2 ZentG kann jede Person vom EDSB resp. EDÖB verlangen, dass er

prüfe, ob bei einer Zentralstelle rechtmässig Daten über sie bearbeitet werden. Die EDSK resp. EDÖK hat die Mitteilung des EDSB resp. EDÖB mit voller Kognition zu überprüfen (Art. 14 Abs. 3 ZentG). Sie ist somit für die Überprüfung solcher Fragen sehr wohl zuständig (vgl. hierzu Grundsatzurteil der EDSK vom 22. Mai 2003/15. März 2004).

d) Zum selben Ergebnis führt eine Überprüfung nach DSG: Nach Art. 4 Abs. 1 DSG dürfen Personendaten nur rechtmässig beschafft werden, und nach Art. 4 Abs. 3 DSG dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Werden Personendaten in JANUS (bzw. wurden sie in seinen Vorgängersystemen) gespeichert, obwohl damit der BStP bzw. das BÜPF verletzt werden, so wurden die Daten rechtswidrig beschafft bzw. liegt eine gesetzwidrige Zweckentfremdung vor. Somit wird durch die Bearbeitung dieser Daten (inkl. deren Speicherung) in JANUS Art. 4 DSG verletzt.

   Die Ausnahme von Art. 2 Abs. 2 Bst. c DSG greift nicht und die Zuständigkeit der EDSK resp. EDÖK kann nicht übergangen werden, wenn Strafverfahren nicht mehr hängig sind oder Daten bearbeitet werden, die rechtswidrig im Strafverfahren beschafft worden sind.

4. Ein weiterer Punkt betrifft die **Bekanntgabe von Personendaten über den Gesuchsteller** durch das Bundesamt. Aus dem Stammdatensatz ergibt sich, dass Daten über den Gesuchsteller an das BAWI bekannt gegeben wurden (Eintrag vom 26.03.97). Das BAP gibt in seinem Bericht vom 30. Januar 2004 (S. 15 f.) an, dem BAWI sei einzig mitgeteilt worden sei, dass es nicht gut wäre, wenn die Schweiz für die Firma D. einen Empfang organisieren würde. Als Rechtsgrundlagen für diese Datenbekanntgabe nennt das BAP Art. 4 Abs. 1 in Verb. mit Bst. d ZentG sowie Art. 13 Abs. 1 ZentG und Art. 6 der ZentV.

   Die ISOK-Verordnung und die Zentralstellenverordnung sind erst auf den 1. Januar 1998 in Kraft getreten. Weil die Datenbekanntgabe offenbar früher, am 26. März 1997 erfolgt war, stellt sich die Frage, ob sie allenfalls direkt auf das am 15. März 1995 in Kraft getretene ZentG gestützt werden konnte.

   Art. 4 Abs. 1 ZentG lautet: "Der Bundesrat regelt für jede Zentralstelle durch Verordnung, unter welchen Voraussetzungen und in welchem Umfang die folgenden Behörden und Amtsstellen zur Zusammenarbeit und fallweisen Auskunft an die Zentralstelle verpflichtet sind." Art. 4 Abs. 1 Bst. d nennt die "Behörden, die für den diplomatischen und konsularischen Verkehr zuständig sind". Art. 13 Abs. 1 ZentG bestimmt: "Die Zentralstelle gibt Personendaten den Behörden im Rahmen der Zusammenarbeitspflicht bekannt. Der Bundesrat bestimmt durch Verordnung, an welche weiteren Empfänger in der Schweiz die Zentralstelle im Einzelfall Personendaten für ein Verfahren weitergeben kann." Die Gesetzmässigkeit der Datenbekanntgabe war ein Hauptanliegen des ZentG (vgl. Botschaft, BBl 1994 I 1163 Ziff. 27).

Die Kompetenz zur Datenbekanntgabe wird in Art. 13 Abs. 1, erster Satz ZentG abhängig gemacht von der Zusammenarbeitspflicht nach Art. 4 Abs. 1 ZentG. Dabei regelt der Gesetzgeber in Art. 4 Abs. 1 die Grundzüge der Zusammenarbeitspflicht und beauftragt den Bundesrat mit den Detailregelungen. In Übereinstimmung mit Art. 17 und Art. 19 DSG sollte die Kompetenz zur Bekanntgabe von Personendaten somit Gegenstand einer generell-abstrakten Regelung sein, welche vom Bundesrat zu erlassen ist. Sofern die Bekanntgabe der Daten über den Gesuchsteller an das BAWI vor dem 1. Januar 1998 erfolgte, stellt sich die Frage, ob eine Datenbekanntgabe vor Erlass der Ausführungsbestimmungen direkt auf diese Bestimmungen des ZentG gestützt werden konnte. Ungeachtet dieser kompetenzrechtlichen Frage ist jedenfalls festzustellen, dass diese Bekanntgabe **nicht zu den gesetzlichen Aufgaben der Zentralstellen** in der Kriminalitätsbekämpfung gehören.

Inhaltlich wurde offenbar zuhanden des BAWI nur die Stellungnahme abgegeben, dass es nicht gut wäre, für die Firma D. einen offiziellen Empfang zu organisieren. Es handelt sich bei einer solchen Stellungnahme von der Zentralstelle zur Bekämpfung des organisierten Verbrechens zweifellos um eine Bekanntgabe von Personendaten. Aus dem Zusammenhang einer solchen Stellungnahme kann der Schluss gezogen werden, dass die Firma D. in Untersuchungen über das organisierte Verbrechen verwickelt ist. Wie weit dem Gesuchsteller Nachteile entstanden sind, weil die Schweiz keinen offiziellen Empfang für die Firma D. organisierte, ist nicht Gegenstand der datenschutzrechtlichen Überprüfung. Die qualifizierende Empfehlung erfüllt aber jedenfalls keinen kriminalpolizeilichen Zweck und war somit nicht rechtmässig.

5. Mit Datum vom 12. März 1999 erstellte das BAP einen analysierenden Bericht über den Gesuchsteller bzw. dessen Firma. Offenbar möchte das BAP diesen **Bericht über den Gesuchsteller als Lage- oder Bedrohungsbericht nach Art. 2 Abs. 1 Bst. c ZentG sehen.** Nach dieser Bestimmung erstellen die Zentralstellen "Lage- und Bedrohungsberichte zuhanden des Eidgenössischen Justiz- und Polizeidepartements (…) und der Strafverfolgungsbehörden". In der Botschaft (BBl 1994 I 1158) wurde dazu ausgeführt:

   "*Die Strafverfolgungsbehörden und übergeordneten politischen Instanzen in Bund und Kantonen müssen über aussagekräftige Informationen verfügen und die Bedrohungslage durch die Aktivitäten des Organisierten Verbrechens zuverlässig einschätzen können. Nur so kann der richtige Entscheid über die Einleitung zweckmässiger Massnahmen getroffen werden. Die Erarbeitung solcher Entscheidgrundlagen obliegt (….) ebenfalls dieser Zentralstelle."*

   Gesetzestext und Materialien deuten eher dahin, dass Lage- und Bedrohungsberichte allgemeinerer Natur sind, und nicht Datenbekanntgaben über bestimmte Personen im Einzelfall. Der Bericht vom 12. März 1999 bezieht sich inhaltlich auf eine konkrete Firma bzw. eine bestimmte Person. Es fragt sich, ob nicht eine Datenbekanntgabe im Einzelfall vorliegt.

Problematisch erscheint die fehlende Abgrenzung zwischen Lage- und Bedrohungsberichten einerseits und Datenbekanntgaben im Einzelfall andererseits auf einer eher strukturellen Ebene: Lage- und Bedrohungsberichte dienen der allgemeinen Orientierung von politischen Entscheidträgern und Strafverfolgungsbehörden. Namentlich die Information von Strafverfolgungsbehörden mittels Lage- und Bedrohungsberichten hat das Ziel, die Strafverfolgung als Ganzes auf aktuelle, besonders gravierende Gefährdungspotenziale auszurichten bzw. zu verhindern, dass einzelne Kantone ihre Strafverfolgung an überholten Bedrohungslagen ausrichten. Dieses Verständnis von Lage- und Bedrohungsberichten liegt auch den Ausführungen des BAP zugrunde (vgl. S. 17 ff. des Berichts vom 30. Januar 2004). Solange Lage- und Bedrohungsberichte eher allgemein gehalten sind, dürften daraus auch keine besonderen Probleme erwachsen. Bezieht sich jedoch ein solcher Bericht ganz konkret nur auf eine bestimmte Person bzw. Firma und wird dieser Bericht dann den Strafverfolgungsbehörden (insbesondere Gerichten und Staatsanwaltschaften) zugeleitet, resultiert daraus eine Folge kaum mehr lösbarer Probleme und Zweifelsfragen: Solche Berichte enthalten tatsächlich, wie das BAP selber ausführt, keine gerichtlich verwertbaren Beweise. Die Berichte dienen nur der Hintergrundinformation der Behörden. Fraglich ist nun, ob solche Berichte in einem konkreten Verfahren zu den Verfahrensakten genommen werden müssen. Auf der einen Seite enthalten sie keine Beweise, auf der anderen Seite aber handelt es sich um Wissen, das dem Gericht oder der Staatsanwaltschaft zur Verfügung steht. Der Anspruch auf rechtliches Gehör nach Art. 29 Abs. 2 BV bzw. die verfassungsrechtlichen Verteidigungsrechte nach Art. 32 Abs. 2 BV müssen eigentlich dazu führen, dass eine angeschuldigte Person solche Berichte einsehen kann (vgl. EGMR Rep. 1997-II, 451 §§ 35 ff., Foucher). Das heisst, die Gerichte und Staatsanwaltschaften müssten angewiesen werden, solche Berichte zu den Akten zu nehmen. Dagegen sprechen natürlich die Geheimhaltungsinteressen im vorliegenden Bereich, und man kann auch anführen, wie das BAP dies tut, dass auf diese Berichte nicht als Beweismittel abgestellt werden kann. Indessen kann man sich mit einigem Recht auf den Standpunkt stellen, dass Richter und Staatsanwalt befangen sind, wenn sie über derartige zusätzliche Geheiminformationen verfügen, die nicht aus den Verfahrensakten ersichtlich sind und welche auch nicht als Beweismittel herangezogen werden. Bloss können die Betroffenen solche Einwände betreffend die Befangenheit des Gerichts schwer geltend machen, weil sie von der Existenz der Geheiminformationen überhaupt keine Kenntnis haben, doch sind deren Sorgen deswegen nicht unmassgeblich (vgl. EGMR Rep. 2003-VI, § 194, Kleyn u.a.; No 41579/98 §§ 67 ff., AB Kurt Kellermann [2004]).

Die Haltung des BAP, wonach es Sache der Strafverfolgungsbehörden sei, die prozessualen Probleme zu lösen, überzeugt nicht, weil davon auszugehen ist, dass die Strafverfolgungsorgane die Geheiminformationen entsprechend den Anweisungen des BAP eben nicht in konkreten Verfahren verwenden und so in Konflikt mit Art. 6 EMRK und Art. 32 BV geraten können.

6. Schliesslich wirft der vorliegende Fall Fragen hinsichtlich der **Aufbewahrung** resp. der **Aufbewahrungsfristen** auf: Nach BGE 120 Ia 147 ff. muss die Aufbewahrungsdauer für erkennungsdienstliche Unterlagen nach der Verdachtslage differenziert ausgestaltet werden (gerichtlich festgestellte "Schuld", Freispruch oder Einstellung mangels Beweisen). Bei festgestellter Unschuld müssten die Daten bzw. Unterlagen sofort gelöscht bzw. vernichtet werden. Bei einer Einstellung des Verfahrens mangels Beweisen erachtet das Bundesgericht eine Aufbewahrungsdauer von ca. fünf Jahren als verhältnismässig.

   Über den Gesuchsteller werden nicht erkennungsdienstliche Unterlagen aufbewahrt, sondern andere polizeiliche Erkenntnisse, wobei aber kein Unterschied zur Aufbewahrung erkennungsdienstlicher Unterlagen ausgemacht werden kann. Die Daten über den Gesuchsteller unterliegen nach Art. 20 JANUS-Verordnung keiner absoluten Aufbewahrungsfrist. Die Regelung von Art. 20 JANUS-Verordnung differenziert nicht, wie vom Bundesgericht verlangt, nach Art und Schwere der Verdachtslage und auch nicht danach, ob ein Strafverfahren eröffnet wurde oder nicht. Über den Gesuchsteller wurden seit dem 7. März 1996 Daten bearbeitet. Seine Daten können mindestens acht Jahre weiterbearbeitet werden. Sofern in der Zwischenzeit ein neuer Vorgang registriert wird, verlängert sich die Aufbewahrungsfrist jeweils um vier Jahre, ohne dass eine absolute Grenze für die zulässige Aufbewahrungsdauer existieren würde. Es scheint fraglich, ob eine solche langjährige Datenbearbeitungs- und Aufbewahrungsdauer im Lichte von Art. 8 EMRK und Art. 13 BV noch verhältnismässig ist, sofern in dieser Zeit die Datenbearbeitung nie zu einer Anklage geführt hat (vgl. EGMR Urteil Amann vom 16. Februar 2000, No.27798/95, Rep. 2000-II, § 78; Urteil Segerstedt-Wiberg u.a. vom 6. Juni 2006, No. 62332/00, §§ 71 ff., bes. § 90). Eine derart lange Aufbewahrungsdauer kann auch, wie das Bundesgericht in BGE 120 Ia 155 festgehalten hat, gegen die verfassungsrechtliche Unschuldsvermutung nach Art. 32 Abs. 1 BV und Art. 6 Abs. 2 EMRK verstossen.

Aus diesen Gründen hat die Eidgenössische Datenschutz- und Öffentlichkeitskommission

festgestellt und empfiehlt:

1. Eine globale Übernahme von Datenbeständen aus alten Informationssystemen in ein neues Informationssystem muss mit Kontrollen der Richtigkeit, insbesondere der Aktualität und Integrität der Personendaten im Einzelfall verbunden werden.

2. Soweit in JANUS noch Personendaten bearbeitet werden, die ungeprüft als gesichert übernommen wurden, ist die Überprüfung der Qualifizierung noch durchzuführen oder die Personendaten sind zu vernichten.

3. Aus Telefonüberwachungen übernommene Personendaten sind ausschliesslich nach Massgabe des BÜPF zu bearbeiten und nicht für beliebige kriminalpolizeiliche Zwecke nach ZentG weiterverwendbar. Die Zuständigkeit des EDÖK als kontrollierendes Gericht umfasst aufgrund von Art. 1 Abs. 2 Bst. c DSG alle Datenbearbeitungen ausserhalb oder nach einem hängigen Strafverfahren sowie Bearbeitungen in Strafverfahren von gesetzwidrig beschafften Personendaten.

4. Datenbekanntgaben an Behörden ausserhalb kriminalpolizeilicher Aufgaben und Zusammenarbeitspflichten nach ZentG sind unzulässig.

5. Über einzelne verdächtige Personen resp. Unternehmen sollten keine geheim zu haltenden Lage- und Bedrohungsberichte verbreitet werden, wenn die empfangenden Strafverfolgungsbehörden nicht die Parteirechte der Betroffenen im Verfahren entsprechend Art. 32 BV und Art. 6 EMRK gewährleisten können.

6. Die Aufbewahrungsregelung nach Art. 20 JANUS-Verordnung ist zu undifferenziert; Art und Schwere der Verdachtslage werden nicht berücksichtigt, ebenso nicht, ob überhaupt ein Strafverfahren eröffnet wurde. Sie kann mit der Zeit unverhältnismässig werden und gegen die verfassungsrechtlichen Unschuldsvermutung nach Art. 32 Abs. 1 BV und Art. 6 Abs. 2 EMRK verstossen.

7. **Eröffnung**
   per l.s. an: EDÖB und fedpol
   Standardmitteilung an Gesuchsteller, vertreten durch RA X.

Eidgenössische Datenschutz- und Öffentlichkeitskommission

Der Sekretär: Der Präsident: